

456-TP-005-001

ECS Project Training Material Volume 5: System Administration

Technical Paper

May 1997

Prepared Under Contract NAS5-60000

RESPONSIBLE ENGINEER

Mike Resnick
EOSDIS Core System Project

Date

SUBMITTED BY

Tom Hickey M&O Deputy Manager
EOSDIS Core System Project

Date

Hughes Information Technology Systems
Upper Marlboro, Maryland

This page intentionally left blank.

Abstract

This is Volume 5 of a series of 10 volumes containing the training material for Pre-Release B Testbed of the Earth Observing System Data and Information System (EOSDIS) Core System (ECS). This lesson provides a detailed description of the process required to perform System Administration tasks.

Keywords: training, system administration, backup, restore, user accounts, access privileges, startup, shutdown, security, workstation, distributed computing environment (DCE), HP OpenView, Networker.

This page intentionally left blank.

Contents

Introduction

Identification.....	1
Scope.....	1
Purpose.....	1
Organization	1

System Administration

Lesson Overview.....	3
Lesson Objectives.....	3
Importance	5

System Startup and Shutdown

Overview.....	7
Cold Startup By Subsystem	7
Warm Startup.....	9
Normal Shutdown	9
Emergency Shutdown	12
System Shutdown by Server	14

Tape Operations

Terminology	15
Networker Administrator Screen.....	15
Labeling Tapes	16
Indexing Tapes	19

System Backups and Restores

Backup Overview	25
Incremental Backup	25
Full System Backup	25
Level 1-9 Backup	25
Special Backups.....	30
Single or Multiple File Restore	32
Complete System Restore.....	36

System Logs

User Administration

Add a New User	43
Deleting a User	47
Changing a User's Password.....	48
Checking File Access Permission.....	49
Changing a File/Directory Access Permission.....	50
Moving a User's Home Directory.....	52

New Workstation Installation

Preparation.....	56
Hardware Preparation	56
Network Configuration.....	56
Installation	56
Hardware.....	56
Operating System Installation.....	57
Software Installation.....	66
Testing and Verification	68
Reboot.....	68
Logging In	69
Test Environment	70

Practical Exercises

System Startup and Shutdown	71
Tape Operations, System Backup and Restore	71
User Administration	71

Slide Presentation

Slide Presentation Description	73
--------------------------------------	----

Figures

1. NSIDC Server Startup Order	7
2. NSIDC Server Shutdown Order	10
3. Networker Administrative main screen	16
4. Jukebox Labeling window	18
5. Tape index following the initial inventory	20
6. Tapes changed but not reinventoried	20
7. Index is updated after reinventory	21
8. Jukebox Mounting window	22
9. Backup Levels Overview	27
10. Networker Scheduler window	28
11. Networker Backup Window	31
12. Networker Recovery Window	34
13. Conflict Resolution window	35
14. Tapes Required for Full System Restore	37
15. Networker Administrator's Window	38
16. User Registration Request Form	43
17. /etc/passwd.yp File Fields	44
18. /etc/group File	44
19. /etc/auto.home File	45
20. Access permissions	50
21. Workstation Installation Steps	55

Tables

1. Backup Levels.....	26
-----------------------	----

Introduction

Identification

Training Material Volume 5 is part of a series of Technical Papers that will be used to teach Maintenance and Operations (M&O) concepts to the M&O staff at the following Distributed Active Archive Centers (DAACs): Langley Research Center (LaRC), National Snow and Ice Data Center (NSIDC) and EROS Data Center (EDC).

Scope

Training Material Volume 5: System Administration defines the steps required to provide the operations staff with sufficient knowledge and information to satisfy all lesson objectives.

This document reflects the August 23, 1995 Technical Baseline maintained by the contractor Configuration Control Board (CCB) in accordance with ECS technical direction #11, dated December 6, 1994.

Purpose

The purpose of this Technical Paper provides a detailed course of instruction that forms the basis for understanding system administration. Lesson objectives are developed and will be used to guide the flow of instruction for this lesson. The lesson objectives will serve as the basis for verifying that all lesson topics are contained within this Student Guide and slide presentation material.

Organization

This document is organized as follows:

- | | |
|---------------------|--|
| Introduction: | The introduction present the document identification, scope, purpose, and organization. |
| Student Guide: | The Student Guide identifies the core elements of this lesson. All Lesson Objectives and associated topics are included. |
| Slide Presentation: | Slide Presentation is reserved for all slides used by the instructor during the presentation of this lesson. |

This page intentionally left blank.

System Administration

Lesson Overview

This lesson will provide you with the tools needed to perform the various tasks required to administer the Pre-Release A Testbed Implementation of the Earth Observing System Data and Information System (EOSDIS) Core System (ECS) during maintenance and operations.

Lesson Objectives

Overall Objective - The overall objective of this lesson is proficiency in the various tasks required to administer the ECS during maintenance and operations.

Condition - The student will be given a copy of *456-TP-005-001 ECS Project Training Material Volume 5: System Administration* and a functioning system.

Standard - The student will use the Procedures Manual in accordance with prescribed methods and complete required procedures without error to accomplish all tasks required.

Specific Objective 1 - The student will startup and shutdown the ECS in its entirety.

Condition - The student will be given a copy of *456-TP-005-001 ECS Project Training Material Volume 5: System Administration* and a functioning system.

Standard - The student will perform without error the procedures required to effect a complete startup and a complete and orderly shutdown of the ECS.

Specific Objective 2 - The student will shutdown and restart a single subsystem of the ECS without affecting other subsystems.

Condition - The student will be given a copy of *456-TP-005-001 ECS Project Training Material Volume 5: System Administration* and a functioning system.

Standard - The student will perform without error the procedures required to effect an orderly shutdown and startup of one subsystem of the ECS without compromising or otherwise affecting the other component subsystems.

Specific Objective 3 - The student will be able to label and index a tape cartridge.

Condition - The student will be given a copy of *456-TP-005-001 ECS Project Training Material Volume 5: System Administration* and a functioning system.

Standard - The student will perform without error the procedures required to label a tape and index a tape cartridge.

Specific Objective 4 - The student will be able to create an incremental tape backup.

Condition - The student will be given a copy of *456-TP-005-001 ECS Project Training Material Volume 5: System Administration* and a functioning system.

Standard - The student will perform without error the procedures required to create an incremental tape backup of system files created or modified within the past six days.

Specific Objective 5 - The student will be able to create a tape backup of the entire ECS system.

Condition - The student will be given a copy of *456-TP-005-001 ECS Project Training Material Volume 5: System Administration* and a functioning system.

Standard - The student will perform without error the procedures required to perform a complete tape backup of the ECS.

Specific Objective 6 - The student will be able to restore individual files or entire volumes of backup tapes to the ECS system.

Condition - The student will be given a copy of *456-TP-005-001 ECS Project Training Material Volume 5: System Administration* and a functioning system.

Standard - The student will perform without error the procedures required to perform individual or complete file restorations.

Specific Objective 7 - The student will be able to review system logs.

Condition - The student will be given a copy of *456-TP-005-001 ECS Project Training Material Volume 5: System Administration* and a functioning system.

Standard - The student will perform without error the procedures required to perform system log maintenance.

Specific Objective 8 - The student will create, modify, and delete user accounts.

Condition - The student will be given a copy of *456-TP-005-001 ECS Project Training Material Volume 5: System Administration* and a functioning system.

Standard - The student will perform without error the procedures required to add a new user account to the ECS, make modifications to a variety of account access parameters, and delete the account from the ECS.

Specific Objective 9 - The student will be able to check and modify access privileges on files and directories across the ECS.

Condition - The student will be given a copy of *456-TP-005-001 ECS Project Training Material Volume 5: System Administration* and a functioning system.

Standard - The student will perform without error the procedures required to check file and directory access privileges and modify them to allow or deny access by various classes of users.

Specific Objective 10 - The student will be able to install, configure, and test a new workstation.

Condition - The student will be given a copy of *456-TP-005-001 ECS Project Training Material Volume 5: System Administration* and a functioning system.

Standard - The student will perform without error the procedures required to install, configure, and test a new workstation including installing COTS, custom software, operating systems.

Importance

A System Administrator's goal is to keep the computer system usable by the users. A system running at peak efficiency does so because of the proper use of the tools provided for and used by the System Administrator. Intimate knowledge of how each tool works and which should be used in a particular situation is crucial to satisfying the ECS user community.

This page intentionally left blank.

System Startup and Shutdown

Overview

Starting or shutting down a computer system may involve nothing more than turning a power switch to the on or off position. However, the interdependency of the various servers may require the System Administrator to startup or shutdown the servers in a particular order. Depending on the situation, the entire computer system may be started or stopped (cold) or only selected servers may be started or stopped (warm). The next sections cover the procedures and details of cold and warm startups and shutdowns.

A complete system startup and shutdown should only need to occur approximately once in three or four months during the early stages of the Pre-Release B Testbed implementation due to the inherent instability of new systems. After the system stabilizes, it is estimated that complete system startups and shutdowns will occur only about once a year. Partial shutdowns and restarts will be performed as needed due to maintenance concerns.

Cold Startup By Subsystem

A cold startup is indicated when there are no subsystems currently running, such as when the system is to be turned on for the first time, following a system maintenance operation that requires all power to be turned off, or following a power failure. In most situations a cold startup is also indicated by the power switch being in the OFF position.

The Cold System Startup is done in sequential order by subsystem. Figure 1 below shows the order at the NSIDC in which each server is to be booted to achieve a fully functional system. A similar order is required at GSFC, LaRC, and EDC.

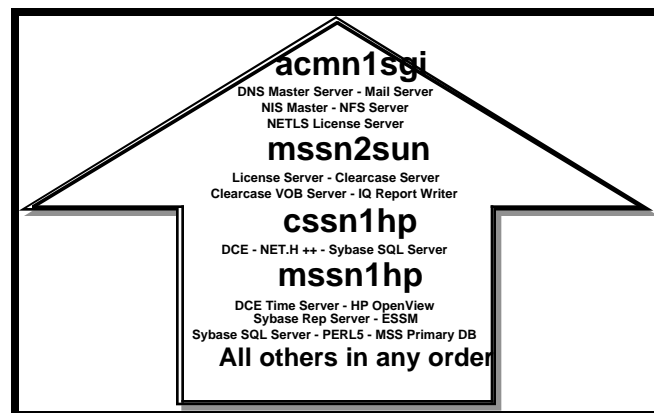


Figure 1. NSIDC Server Startup Order

Cold Subsystem Startup Procedure

- 1 Determine which machines perform the following functions. Some may perform multiple functions:
 - Domain Name Server (DNS) Master
 - Name Information Server (NIS) Master
 - Mail Hub Server(s)
 - Automount Servers
 - Clearcase Server
 - Communication Subsystem (CSS) including Distributed Computing Environment (DCE) Server
 - DCE License Server for SUN
 - Other License Servers
 - System Management Subsystem
 - Sybase SQL Servers
 - Data Server Subsystem (DSS)
 - Planning & Data Processing System (PDPS)
 - Client, Interoperability and Data Management (CIDM) Subsystem
 - 2 Startup the DNS Master. Once the system has booted without error, proceed to step 3.
 - 3 Power on the NIS Master. Once the system has booted without error, proceed to step 4.
 - 4 Power on the Mail Hub server(s). Once the system(s) have booted without error, proceed to step 5.
 - 5 Power on the Automount/Mail HUB server(s). Once the system(s) have booted without error, proceed to step 6.
 - 6 Power on the Clearcase server(s). Once the systems(s) have booted without error, proceed to step 7.
 - 7 Power on the CSS server(s). Once the system(s) have booted without error, proceed to step 8.
 - 8 Power on the DCE License server for SUN. Once the system has booted without error, proceed to step 9.
 - 9 Power on the Other License server(s). Once the system(s) have booted without error, proceed to step 10.
 - 10 Power on the MSS server(s). Once the system(s) have booted without error, proceed to step 11.
 - 11 Power on the DSS server(s). Once the system(s) have booted without error, proceed to step 12.
 - 12 Power on the PDPS server(s). Once the system(s) have booted without error, proceed to step 13.
 - 13 Power on the CIDM server(s).
-

Warm Startup

A warm startup is indicated when there are some subsystems currently running while others have been shutdown either due to operator intervention or an external malfunction. The subsystems not actively running need to be started without interfering with the current active operations. In some instances, a warm startup may require some active subsystems to be shutdown and restarted so that their interaction and connectivity will be properly resumed.

Warm Subsystem Startup Procedure

- 1 Determine which machines perform the following functions:
 - Domain Name Server (DNS) Master
 - Name Information Server (NIS) Master
 - Mail Hub Server(s)
 - Automount Servers
 - Clearcase Server
 - Communication Subsystem (CSS) including Distributed Computing Environment (DCE) Server
 - DCE License Server for SUN
 - Other License Servers
 - System Management Subsystem
 - Sybase SQL Servers
 - Data Server Subsystem (DSS)
 - Planning & Data Processing System (PDPS)
 - Client, Interoperability and Data Management (CIDM) Subsystem
 - 2 Determine which machine is currently down.
 - 3 Determine the interoperability dependencies among the machines.
 - 4 Turn on machines in an order consistent with the dependencies.
-

Normal Shutdown

A normal shutdown occurs when the operator is required to turn off the power to the entire system or any of the component subsystems. Normal shutdowns are scheduled by the Resource Manager with prior approval by the DAAC management at a time that minimizes disruption to system users, usually during off hours. No loss of data is anticipated from a normal shutdown. All subsystems are shutdown in a routine and normal fashion.

The system shutdown procedure is performed by the System Administrator at the discretion of the Network Administrator, usually for the purpose of repair. The system shutdown is normally performed in reverse order of the system startup. Figure 2 below shows the order at the NSIDC in which each server is to be shutdown to achieve an orderly shutdown. A similar order is required at GSFC, LaRC and EDC.

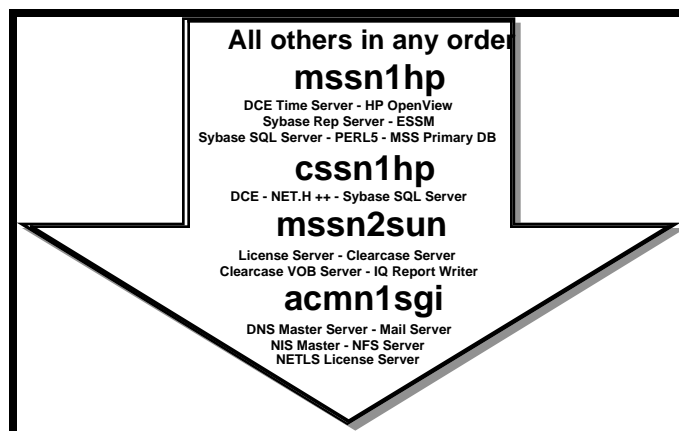


Figure 2. NSIDC Server Shutdown Order

The System Administrator must be logged in as root to perform a shutdown.

Prior to a normal shutdown, the System Administrator sends broadcast messages to all Computer Operators on the system at Shutdown Minus 30 minutes, Shutdown Minus 15 minutes, and Shutdown Minus 1 minute. At the scheduled shutdown time, the System Administrator blocks all incoming requests from the gateway and allows active jobs to complete (unless it is anticipated that they will take longer than 10 minutes in which case the System Administrator will terminate the processes and notify the originator). The System Administrator then begins to shut down all subsystems the order prescribed in the procedure below.

HP OpenView is used as the monitoring agent with each subsystem icon turning red as it is successfully shutdown. When all subsystems have been successfully shutdown, the UNIX prompt appears on the console screen. Total time from shutdown initiation to completion may be as long as 45 minutes.

Normal Shutdown By Subsystem Procedure

Steps A-G below are preliminary steps to shutting down each subsystem.

- A** Login to the server as **root**.
- B** Enter root password.

- C** Type **wall** and press **Return**.
- D** Type **This machine is being shutdown for *reason*. Please save your work and log off now. We are sorry for the inconvenience.** Press Control and D keys simultaneously.
- E** Wait at least five minutes.
- F** Type **shutdown -g0 -i0** or **shutdown now -i0** at the UNIX prompt and press **Return**.
- G** Power off all peripherals and the CPU.
- 1** Determine which machines perform the following functions:
- DNS Master
 - NIS Master
 - Mail Hub Server(s)
 - Automount Server
 - Clearcase Server
 - CSS including DCE Server
 - DCE License Server for SUN
 - Other License Servers
 - MSS including Tivoli Server and Sybase SQL Servers
 - DSS
 - Ingest
 - PDPS
 - CIDM
- 2** Power off the CIDM server(s) by following steps A-G above for each machine. Once the system(s) have shutdown without error, proceed to step 3.
- 3** Power off the PDPS server(s) by following steps A-G above for each machine. Once the system(s) have shutdown without error, proceed to step 4.
- 4** Power off the Ingest server(s) by following steps A-G above for each machine. Once the system(s) have shutdown without error, proceed to step 5.
- 5** Power off the DSS server(s) by following steps A-G above for each machine. Once the system(s) have shutdown without error, proceed to step 6.
- 6** Power off the MSS server(s) by following steps A-G above for each machine. Once the system(s) have shutdown without error, proceed to step 7.
- 7** Power off the Other License server(s) by following steps A-G above for each machine. Once the system(s) have shutdown without error, proceed to step 8.
- 8** Power off the DCE License server for the SUN by following steps A-G above for each machine. Once the system(s) have shutdown without error, proceed to step 9.
- 9** Power off the CSS server(s) by following steps A-G above for each machine. Once the system(s) have shutdown without error, proceed to step 10.
- 10** Power off the Clearcase server(s) by following steps A-G above for each machine. Once the system(s) have shutdown without error, proceed to step 11.

- 11** Power off the Automount server(s) by following steps A-G above for each machine. Once the system(s) have shutdown without error, proceed to step 12.
 - 12** Power off the Mail Hub server(s) by following steps A-G above for each machine. Once the system has shutdown without error, proceed to step 13.
 - 13** Power off the NIS Master by following steps A-G above for each machine. Once the system has shutdown without error, proceed to step 14.
 - 14** Power off the DNS Master.
-

Emergency Shutdown

An emergency shutdown is indicated when the System Administrator determines that the entire system or a component subsystem requires immediate maintenance. Indications that an emergency shutdown is in order include:

- the system or subsystem is locked up and users are unable to access or maneuver through the system
- an impending or actual power failure
- an actual system or subsystem hardware or software failure

Every effort should be made to minimize loss of data during an emergency shutdown by informing users to save files and log off if at all possible. However, circumstances may be such that a large-scale loss of data is unavoidable. In such instances, data will be restored from the most recent backup tapes and temporary backup files provided by the system (if applicable).

If the entire system is locked up then a complete system shutdown is required and the emergency shutdown and start-up procedures should be executed immediately. The DAAC manager is notified after the system has been brought back on line.

If major subsystems are locked up then a complete system shutdown is required and the emergency shutdown and start-up procedures should be executed immediately. The DAAC manager is notified after the system has been brought back on line.

If one or only a few of the subsystems are experiencing problems and only some of the users are impacted, the subsystem problem(s) should be resolved first. If after all efforts to resolve the subsystem problems are exhausted the System Administrator determines that a shutdown is necessary, only those affected subsystems should be shutdown. Only if these steps provide no relief should the entire system be brought down. In any case, every effort should be made not to impact users that are still on the system and to minimize data loss.

Emergency Shutdown Procedure

- 1 Login to the server as root.
 - 2 Enter root password.
 - 3 Type **sync** at the UNIX prompt, then press **Return**.
 - **sync** causes all information in memory that should be on disk to be written out including modified super blocks, modified inodes, and delayed block I/O. If the system is to be stopped, sync must be called to insure file system integrity.
 - 4 Type **sync** again at the UNIX prompt, then press **Return**.
 - 5 Type **halt** at the UNIX prompt, then press **Return**.
 - 6 Shutdown all client workstations.
 - 7 Determine which machines perform the following functions. Some machines may perform multiple functions:
 - Sybase SQL/Rep
 - Autosys
 - Clearcase
 - Tivoli
 - DCE
 - Automount
 - Mail Hub
 - NIS
 - DNS
 - 8 Power off the Sybase SQL/Rep server(s). Once the system has shutdown without error, proceed to Step 9.
 - 9 Power off the Autosys server(s). Once the system has shutdown without error, proceed to Step 10.
 - 10 Power off the Clearcase server(s). Once the system has shutdown without error, proceed to Step 11.
 - 11 Power off the Tivoli server(s). Once the system has shutdown without error, proceed to Step 12.
 - 12 Power off the DCE server(s). Once the system has shutdown without error, proceed to Step 13.
 - 13 Power off the Automount server(s). Once the system has shutdown without error, proceed to Step 14.
 - 14 Power off the NIS server(s). Once the system has shutdown without error, proceed to Step 15.
 - 15 Power off the DNS server(s).
-

In case of EXTREME emergency where time does not allow you to execute the above procedures, execute the procedure steps that follow. Be forewarned, however, that this procedure does not ensure file system integrity and will result in loss of data and/or damage to the file system. It should be used only as a last resort.

Extreme Emergency System Shutdown Procedure

- 1 At the **Login:** prompt, type **root**, then press **Return**.
- 2 At the **Password:** prompt, enter the **RootPassword**.
- 3 Press the **L1** and the **a** keys simultaneously.
- 4 Once returned to an **ok** or **>** prompt, turn the power switches on the CPU and all peripherals to the **off** position.

WARNING

The use of L1-a does not ensure file system integrity. There is a very high risk of losing data when this process is used.

System Shutdown by Server

In situations where only a single server requires maintenance the System Administrator will need to determine if and how the faulty server affects other servers on the network. One server may be able to be shutdown without affecting the rest of the network, or several dependent servers may have to be shutdown in addition to the target server. Because of these interdependencies, each case will have to be uniquely evaluated.

Tape Operations

In this lesson you will learn how Networker Administrative software and the Exabyte tape drive work together to administer the use of tapes for system backups and file restorations. Functions such as how to label a new tape, how to index a tape cartridge, and how to perform backups and restores are covered.

Terminology

- **Cartridge** - A hardware device that is part of the Exabyte tape drive. It holds up to 10 tapes that are automatically selected by Networker.
- **Drive** - Hardware device into which the tape or tape cartridge is inserted that performs the actual recording of data.
- **Index** - A list of the labeled tapes currently stored in the jukebox.
- **Inventory** - The action of making an **index**.
- **Jukebox** - A hardware device that stores more than one tape used for system backups and restores. Working in conjunction with specialized software, it can automatically select the proper tape, load the tape into the tape drive, and return it to its appropriate slot upon completion of the task.
- **Label** - A unique name assigned to a tape by Networker.
- **Volume** - A recording medium; in the case of this course, a volume and a tape are synonymous.

Networker Administrator Screen

The main Networker Administrator screen (Figure 3), which is displayed after typing **nwadmin** at a UNIX prompt, contains four main sections.

- The menu bar at the top of the screen, which displays all of the possible capabilities of Networker Admin..
- The **speedbar**, which can be customized, displays icons which execute the most common procedures.
- Current configuration information, including the current Networker server, the available backup devices (tape drives, file systems, CD-ROMs, etc.).
- Current status windows which display in real time the actual activity on the various devices, and progress and error messages.

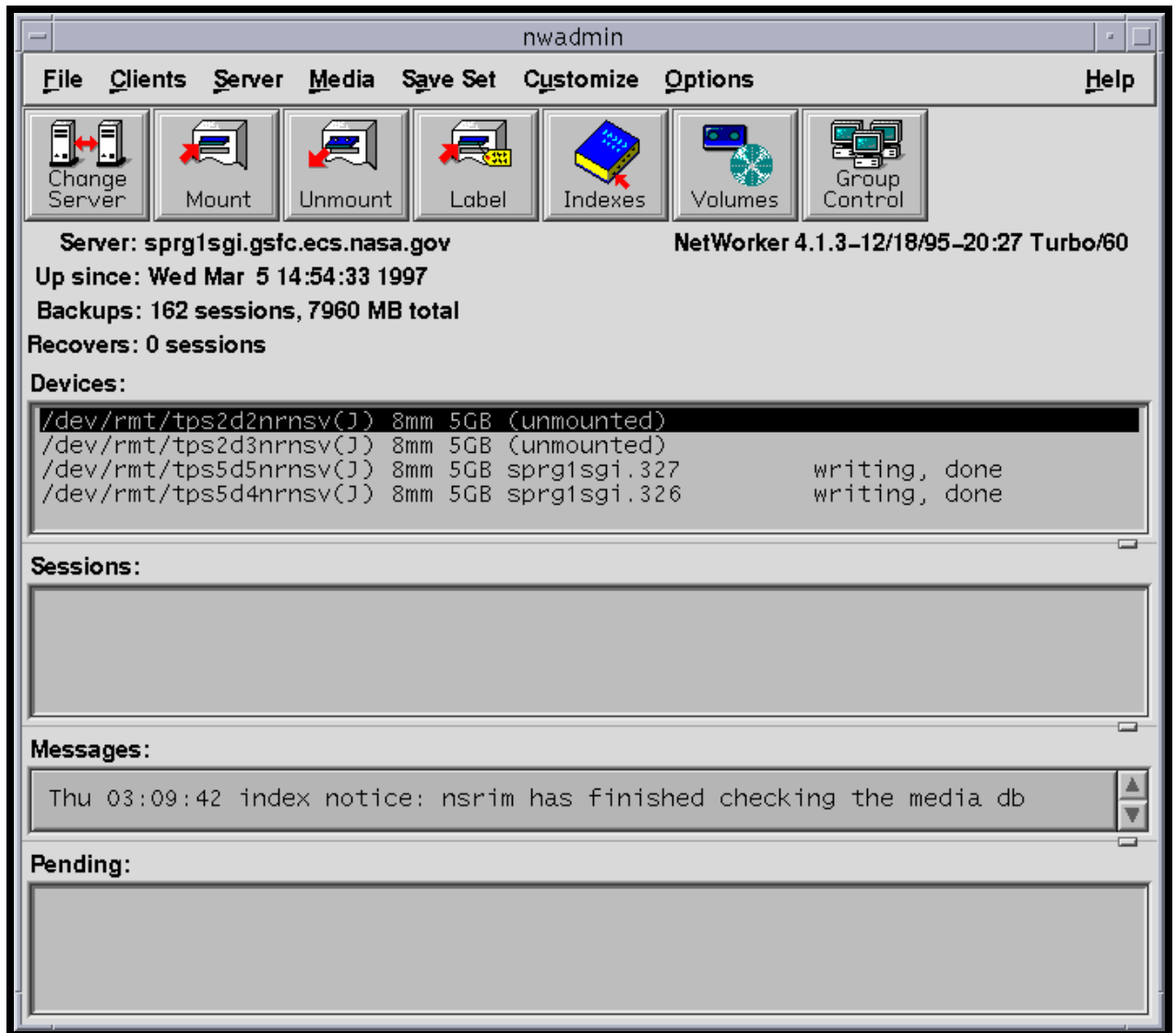


Figure 3. NetWorker Administrative main screen

Labeling Tapes

Files and directories have unique names that are assigned by the user to identify them. In much the same manner, tapes are given unique names, or labels. This allows such programs as NetWorker and such hardware devices such as the Exabyte jukebox to automate the tape selection process when performing system backups and restores. When a tape is initialized, NetWorker assigns it a label. NetWorker then stores the tape's label with a file that is written to the tape so that when a file restoration request is received, NetWorker will know exactly which tape to select from the jukebox.

Tape Labeling Procedure

- 1 Log into the backup server by typing: **telnet *BackupServerName*** or **rsh *BackupServerName*** at the UNIX prompt, then press **Return**.
- 2 If a **Login:** prompt appears, log in as yourself by typing: ***YourUserID***, then press **Return**.
 - A password prompt is displayed.
- 3 Enter ***YourPassword***, then press **Return**.
 - Remember that ***YourPassword*** is case sensitive.
 - You are authenticated as yourself and returned to the UNIX prompt.
- 4 Log in as root by typing: **su**, then press **Return**.
 - A password prompt is displayed.
- 5 Enter the ***RootPassword***, then press **Return**.
 - Remember that ***YourPassword*** is case sensitive.
 - You are authenticated as yourself and returned to the UNIX prompt.
- 6 Set display to current terminal by typing: **setenv DISPLAY *IPNumber:0.0*** or **setenv DISPLAY *BackupServerName:0.0***, then press **Return**.
- 7 At the UNIX prompt, type **nwadmin**, then press **Return**.
 - A window opens for the Networker Administrative program.
- 8 Insert the blank tape(s) in the jukebox's cartridge, then install the cartridge in the jukebox.
 - Remove any non-blank tapes from the cartridge or else they will be re-labeled and the data on the tapes will be lost.
- 9 Click the **Label** button.
 - The **Jukebox Labeling** window opens (Figure 4).

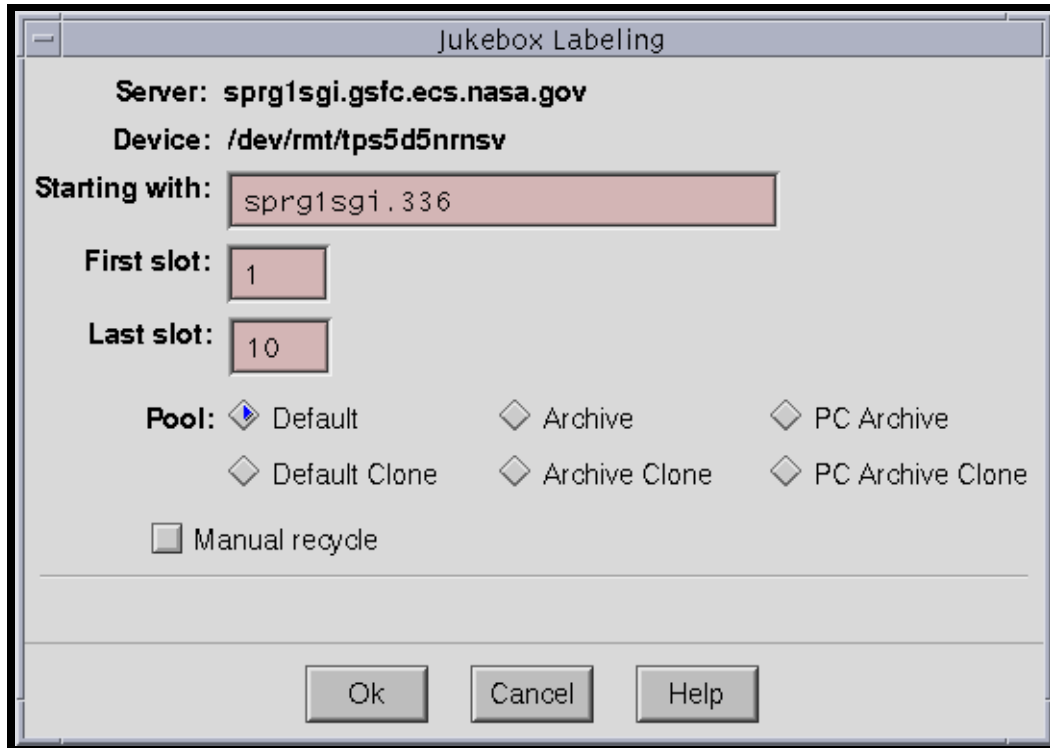


Figure 4. Jukebox Labeling window.

- 10 In the field marked **Starting with**, enter the tape label you wish to use for the first tape in the sequence.
 - Tape labels are named by using the host name (e.g., **sprn1sgi**), a dot or period, and a sequential number (e.g., **001**, **002**).
 - By default, the system will prompt you with the next label in the sequence (e.g., **sprn1sgi.011**).
- 11 In the **First Slot** field, enter **1** or the slot containing the first volume to be labeled; in the **Last Slot** field, enter **10** or the slot containing the last volume to be labeled.
 - Slot 1 is at the top of the cartridge and 10 at the bottom.
 - Slot 11 is the non-removable slot within the jukebox. This usually contains a cleaning tape.
 - It is OK to leave empty slots.
- 12 Click the **OK** button.
 - A status message indicating the progress of the tape labeling procedure appears and updates.
 - Labeling a full cartridge of tapes takes about 15 minutes.

- 13 When the status in the **Jukebox Labeling** window reads **finished**, click the **Cancel** button.
 - The **Jukebox Labeling** window closes.
 - 14 From the **File** menu, select **Exit**.
 - The **nwadmin** program terminates and you are returned to the UNIX prompt.
 - 15 At the UNIX prompt for the backup server, type **exit**, then press **Return**.
 - **Root** is logged out.
 - 16 Type **exit** again, then press **Return**.
 - You are logged out of and disconnected from the backup server.
 - 17 Put an identifying sticker on the outside of each tape cassette.
-

Indexing Tapes

Labeled tapes are loaded in a tape cartridge that is inserted into the Exabyte tape drive, also referred to as the *jukebox*. Networker needs to know the location of each tape in the jukebox. To do this, Networker uses a process called **inventory** which prepares an index by matching a tape label to the cartridge slot that holds that tape (Figure 5). Then, when a request to recover a file or a set of files is received, *Networker* locates the tape based on the information in its memory.

CAUTION

If you move a tape from its position in the cartridge, Networker will not know where to find it (Figure 6). You must re-index the cartridge by performing these procedures again. Otherwise Networker will not select the correct tape (Figure 7).

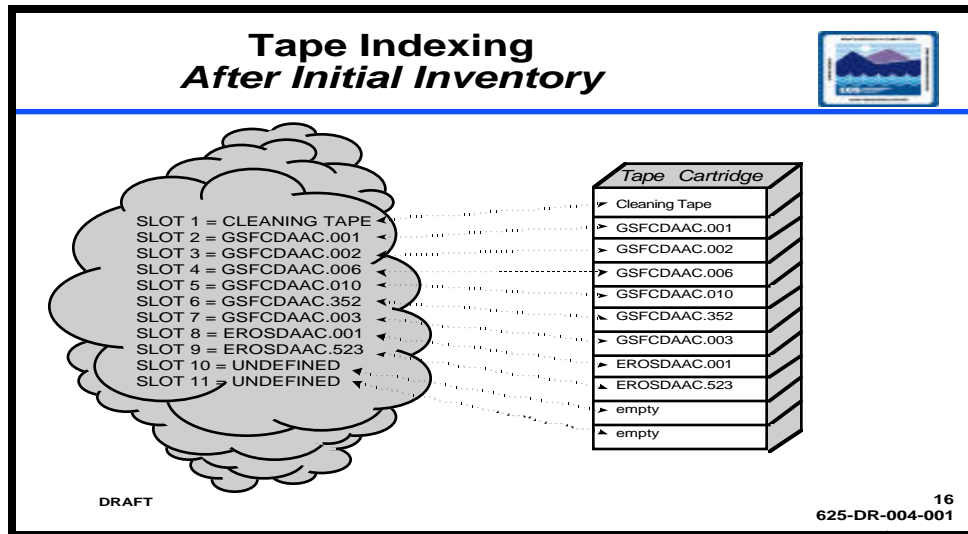


Figure 5. Tape index following the initial inventory.

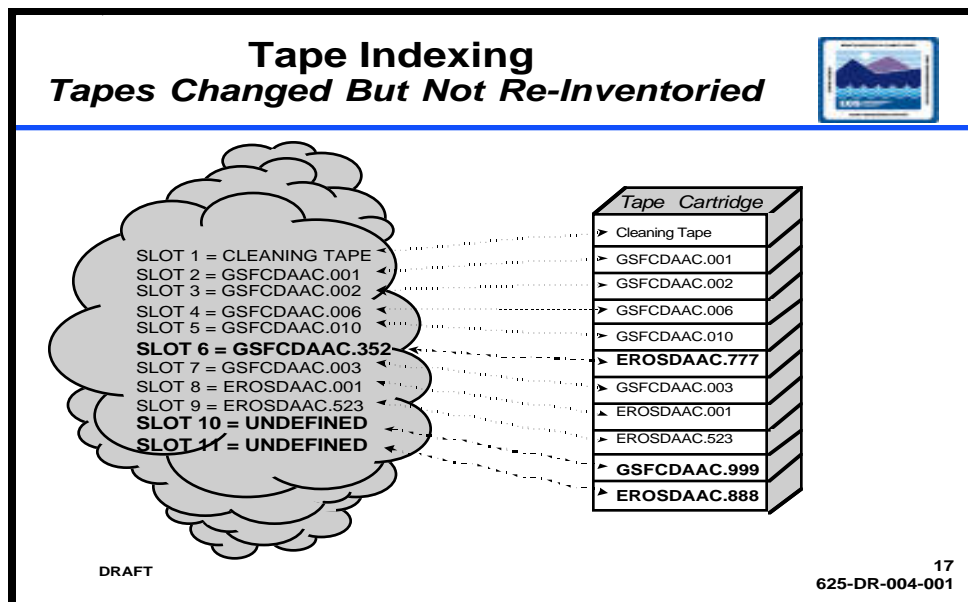


Figure 6. Tapes changed but not reinventoried.

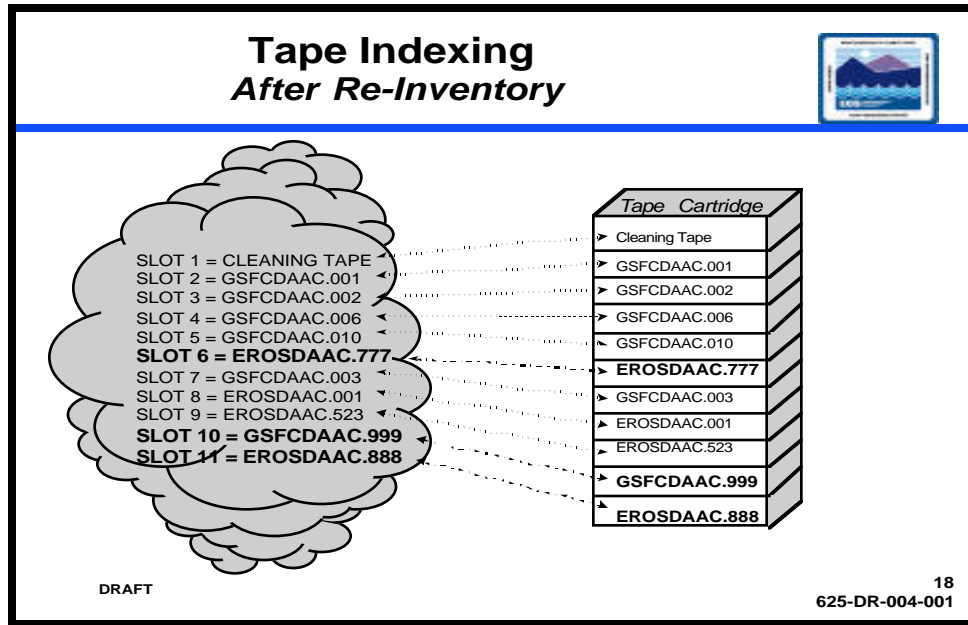


Figure 7. Index is updated after reinventory.

Indexing Tapes Procedure

- 1 Log into the backup server by typing: **telnet BackupServerName** or **rsh BackupServerName** at the UNIX prompt; then press **Return**.
- 2 If a **Login:** prompt appears, log in as yourself by typing: **YourUserID**, then press **Return**.
 - The password prompt is displayed.
- 3 Type **YourPassword**, then press **Return**.
 - Remember that your password is case sensitive.
 - You are authenticated as yourself and returned to the UNIX prompt.
- 4 Log in as root by typing **su**, then press **Return**.
 - A password prompt is displayed.
- 5 Enter the **RootPassword**, then press **Return**.
 - You are authenticated as root and returned to the UNIX prompt.
- 6 Set display to current terminal by typing: **setenv DISPLAY IPNumber:0.0** or **setenv DISPLAY BackupServerName:0.0**, then press **Return**.
- 7 At the UNIX prompt, type **nwadmin**, then press **Return**.
 - A window opens for the **Networker Administrative** program.

- 8 Click the **Mount** button, or select **Media -> Mount** from the menu.
- The **Jukebox Mounting** window opens (Figure 8) and displays a list of the tapes that Networker is currently aware of.
 - When you are finished with this window, click the **Cancel** button.

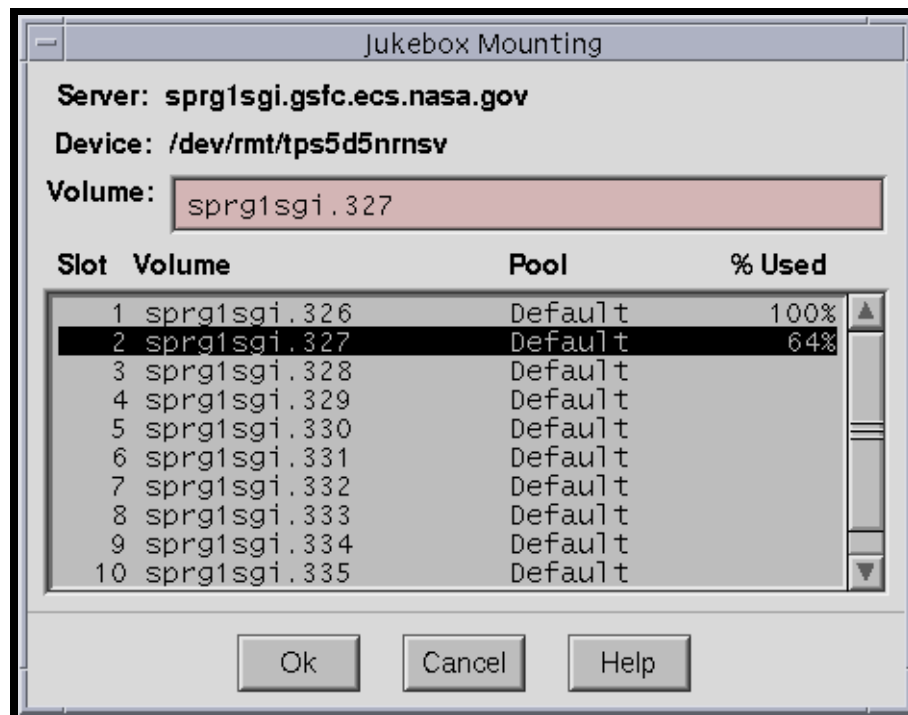


Figure 8. Jukebox Mounting window.

- 9 Insert the required tape(s) in the jukebox's cartridge, then install the cartridge in the jukebox.
- Refer to the jukebox's documentation for detailed instructions on installing the cartridge.
- 10 Select **Media** from the menu bar, then select **Inventory**.
- The **Jukebox Inventory** window opens.
- 11 In the **First Slot** field, enter **1** or the slot containing the first volume to be labeled; in the **Last Slot** field, enter **10** or the slot containing the last volume to be labeled.
- Slot 1 is at the top of the cartridge and 10 at the bottom.
 - Slot 11 is the non-removable slot within the jukebox. This usually contains a cleaning tape.
 - It is OK to leave empty slots or slots with previously inventoried tapes.

- 12** Click the **OK** button.
- A status message indicating the progress of the tape indexing procedure appears and updates.
 - Inventorying a full cartridge of tapes takes between 20 and 30 minutes.
- 13** When the **Jukebox Inventory** status reads **finished**, click the **Cancel** button.
- 14** Click the **Mount** button to verify that the indexing worked.
- The **Jukebox Mounting** window opens.
 - The **required tape(s)** should be shown. If not, repeat this procedure from step 8.
- 15** Click the **Cancel** button.
- The **Jukebox Mounting** window closes.
- 16** From the menu bar, select **File**, then select **Exit**.
- 17** At the UNIX prompt for the *BackupServer*, type **exit**, then press **Return**.
- 18** At the next UNIX prompt, type **exit** again, then press **Return**.
-

This page intentionally left blank.

System Backups and Restores

Backup Overview

Performing regular and comprehensive backups is one of the most important responsibilities a System Administrator has. Backups are the insurance that essentially all of the system data is always available. In cases of catastrophic system failure, where the system crashes and all disks are damaged, the System Administrator should be able to restore virtually all of the data from the backup tapes.

Networker supports three types of backups that can be run automatically according to a pre-programmed schedule:

- Incremental
- Full
- Level 1-9

On-demand backups can also be run through Networker with System Administrator intervention.

This chapter explains the three types of backups, how Networker is programmed to perform the backups, and how the System Administrator can override the schedule to perform on-demand backups.

Incremental Backup

An incremental backup copies to tape all files on a system or subsystem that were created or modified since the previous incremental backup regardless of the backup level. The purpose of an incremental backup is to insure that the most recent edition of a file is readily available in case user error or disastrous system failure causes the file to become corrupt. Incremental backups are scheduled at a time that causes minimal disruption to the users. Copies of all incremental backup tapes are stored offsite for five weeks before they are reused.

Full System Backup

A full system backup is a snapshot of the data on the entire system as of a particular date. The data is stored on tapes that are used to recreate the system in the event of a catastrophic system failure. The full system backup is automatically run by Networker on a regular schedule, usually monthly. Copies of all full backup tapes are stored offsite for security purposes.

Level 1-9 Backup

Because of the enormous amount of data that will reside on the ECS, full system backups will eventually require a proportionally enormous number of backup tapes, which will become cumbersome to administer from both a logistical and an economic standpoint. Therefore, Networker employs a 9-level hierarchy that combines true full system backups, true incremental

backups, and partial backups to create an economically feasible snapshot of the system. The levels are explained in Table 1 and Figure 9 below:

Table 1. Backup Levels

LEVEL	EXPLANATION
0	Full system backup selects every file on the system regardless of creation or modification date.
1	Selects all files created or modified since the last full backup.
2	Selects all files created or modified since the last level 1 backup, or in the absence of a level 1 backup, since the last level 0 backup.
3	Selects all files created or modified since the last level 2 backup, or in the absence of a level 2 backup, since the last level 1 backup, or in the absence of a level 1 backup, since the last level 0 backup.
4	Selects all files created or modified since the last level 3 backup, or in the absence of a level 3 backup, since the last level 2 backup, or in the absence of a level 2 backup, since the last level 1 backup, or in the absence of a level 1 backup, since the last level 0 backup.
5	Selects all files created or modified since the last level 4 backup, or in the absence of a level 4 backup, since the last level 3 backup, or in the absence of a level 3 backup, since the last level 2 backup, or in the absence of a level 2 backup, since the last level 1 backup, or in the absence of a level 1 backup, since the last level 0 backup.
6	Selects all files created or modified since the last level 5 backup, or in the absence of a level 5 backup, since the last level 4 backup, or in the absence of a level 4 backup, since the last level 3 backup, or in the absence of a level 3 backup, since the last level 2 backup, or in the absence of a level 2 backup, since the last level 1 backup, or in the absence of a level 1 backup, since the last level 0 backup.
7	Selects all files created or modified since the last level 6 backup, or in the absence of a level 6 backup, since the last level 5 backup, or in the absence of a level 5 backup, since the last level 4 backup, or in the absence of a level 4 backup, since the last level 3 backup, or in the absence of a level 3 backup, since the last level 2 backup, or in the absence of a level 2 backup, since the last level 1 backup, or in the absence of a level 1 backup, since the last level 0 backup.
8	Selects all files created or modified since the last level 7 backup, or in the absence of a level 7 backup, since the last level 6 backup, or in the absence of a level 6 backup, since the last level 5 backup, or in the absence of a level 5 backup, since the last level 4 backup, or in the absence of a level 4 backup, since the last level 3 backup, or in the absence of a level 3 backup, since the last level 2 backup, or in the absence of a level 2 backup, since the last level 1 backup, or in the absence of a level 1 backup, since the last level 0 backup.
9	Selects all files created or modified since the last level 8 backup, or in the absence of a level 8 backup, since the last level 7 backup, or in the absence of a level 7 backup, since the last level 6 backup, or in the absence of a level 6 backup, since the last level 5 backup, or in the absence of a level 5 backup, since the last level 4 backup, or in the absence of a level 4 backup, since the last level 3 backup, or in the absence of a level 3 backup, since the last level 2 backup, or in the absence of a level 2 backup, since the last level 1 backup, or in the absence of a level 1 backup, since the last level 0 backup.

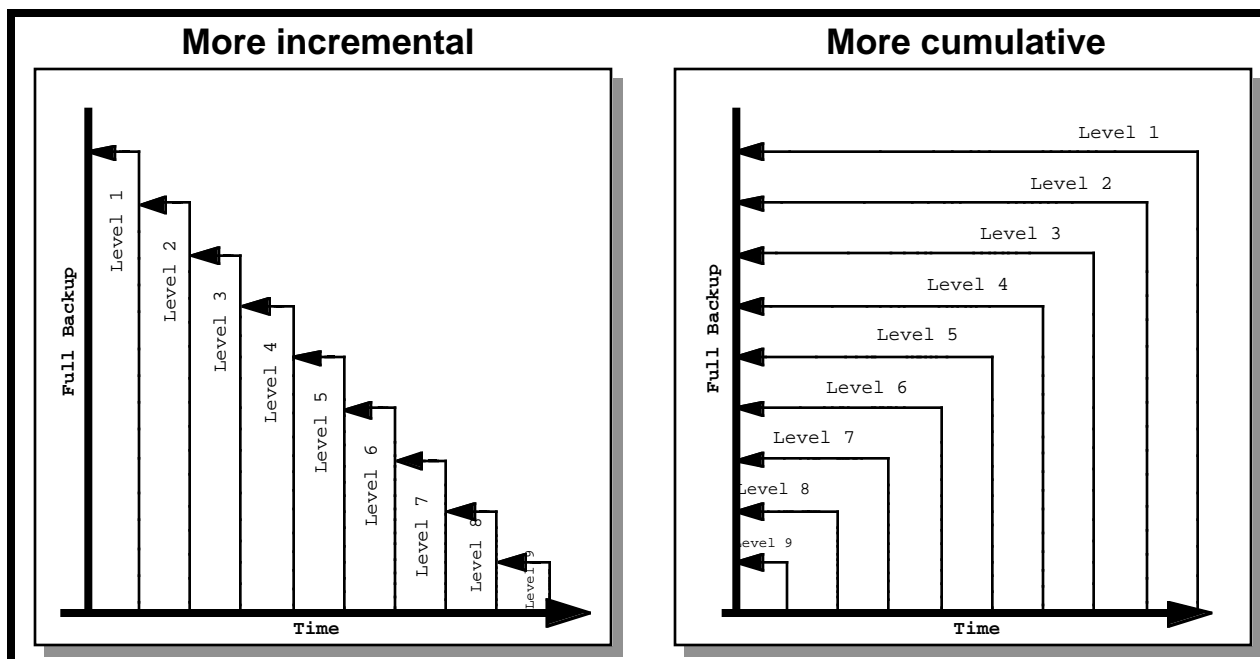


Figure 9. Backup Levels Overview

All backups, whether scheduled or on-demand, are performed using Networker via the **Networker Schedules** windows (Figure 10).

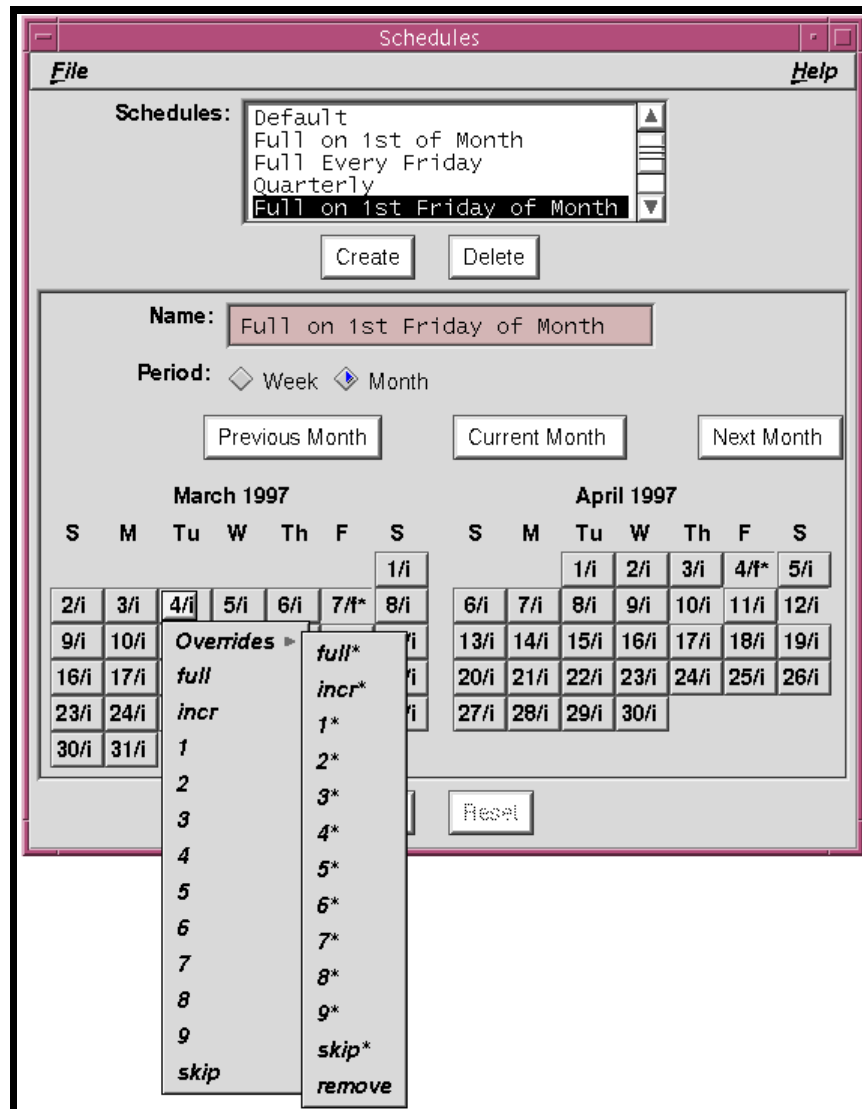


Figure 10. Networker Scheduler window.

Backup Scheduling Procedure

- 1 Log into the machine to be backed up by typing: **telnet *BackedUpSystemName*** or **rsh *BackedUpSystemName***, then press **Return**.
- 2 If a **Login:** prompt appears, log in as yourself by typing: ***YourUserID***, then press **Return**.
 - A password prompt is displayed.
- 3 Enter ***YourPassword***, then press **Return**.
 - Remember that ***YourPassword*** is case sensitive.

- You are authenticated as yourself and returned to the UNIX prompt.
- 4** Log in as root by typing: **su**, then press **Return**.
 - A password prompt is displayed.
- 5** Enter the **RootPassword**, then press **Return**.
 - Remember that **YourPassword** is case sensitive.
 - You are authenticated as yourself and returned to the UNIX prompt
- 6** Set display to current terminal by typing: **setenv DISPLAY IPNumber:0.0** or **setenv DISPLAY BackupServerName:0.0**, then press **Return**.
- 7** At the UNIX prompt, type **nwadmin**, then press **Return**.
 - A window opens for the Networker Administrative program.
- 8** Go to the **Customize** menu, select **Schedules**.
 - The **Schedules** window opens (Figure 10).
 - The calendar date buttons include the date, a slash, and either a letter or a number.
 - An **i** after the slash stands for incremental, indicating that an incremental backup is scheduled for that day.
 - An **f** after the slash stands for full, indicating that a full system backup is scheduled for that day.
 - A **number** after the slash indicates the backup level that is scheduled for that day.
- 9** To permanently change the backup type for a particular day, click and hold the button for that day, then select the desired backup type from the resulting menu. Skip to step 11.
- 10** To temporarily change the backup type for a particular day, click and hold the button for that day, then select **Overrides** from the resulting menu, then select the desired backup type from the resulting menu. Continue with step 11.
- 11** Click the **Apply** button.
- 12** Close the **Schedules** window by clicking in the upper left corner of the **Schedules** window and selecting **Close** from the resulting menu.
- 13** Click the **Group Control** button.
 - The **Group Control** window opens.
- 14** Click the **Start** button.
 - A **Notice** window opens.
- 15** Click the **OK** button.
 - The **Notice** window closes.

- The regularly scheduled backup will still run (even though we are now doing a backup).
- 16 Close the **Group Control** window by clicking in the upper left corner of the **Group Control** window and selecting **Close** from the resulting menu.
 - Status updates appear in the **nwadmin** window.
 - When the backup is complete, a **Finished** message will appear.
 - 17 If the button for today in step 9 had an i on it, go to step 22.
 - 18 Go to the **Customize** menu, select **Schedules**.
 - The Schedules window opens.
 - 19 Click and hold the button for today, select **Overrides** from the resulting menu, select **Full** from the next resulting menu.
 - 20 Click the **Apply** button.
 - 21 Close the **Schedules** window by clicking in the upper left corner of the **Schedules** window and selecting **Close** from the resulting menu.
 - 22 Select **Exit** from the **File** menu to quit the Networker Administrative program.
 - The **nwadmin** window closes.
 - 23 At the UNIX prompt for the machine to be backed up, type **exit**, then press **Return**.
 - Root is logged out.
 - 24 Type **exit** again, then press **Return**.
 - You are logged out and disconnected from the machine to be backed up.
-

Special Backups

In addition to the incremental, full, and level backups described, an individual may request a special backup of specific files. This can be accomplished using the special backups procedure that follows.

Special Backup Procedure

- 1 Log into the machine to be backed up by typing: **telnet *BackedUpSystemName*** or **rsh *BackedUpSystemName***, then press **Return**.
- 2 If a **Login:** prompt appears, log in as yourself by typing: ***YourUserID***, then press **Return**.
 - A password prompt is displayed.
- 3 Enter ***YourPassword***, then press **Return**.
 - Remember that ***YourPassword*** is case sensitive.

- You are authenticated as yourself and returned to the UNIX prompt.
- 4 Log in as root by typing: **su**, then press **Return**.
- A password prompt is displayed.
- 5 Enter the **RootPassword**, then press **Return**.
- Remember that **YourPassword** is case sensitive.
 - You are authenticated as yourself and returned to the UNIX prompt.
- 6 Set display to current terminal by typing: **setenv DISPLAY IPNumber:0.0** or **setenv DISPLAY BackedUpSystemName:0.0**, then press **Return**.
- 7 Execute the Networker Backup program by entering: **nwbackup**, then press **Return**.
- A **Networker Backup** window opens (Figure 11). You are now able to perform a full backup.

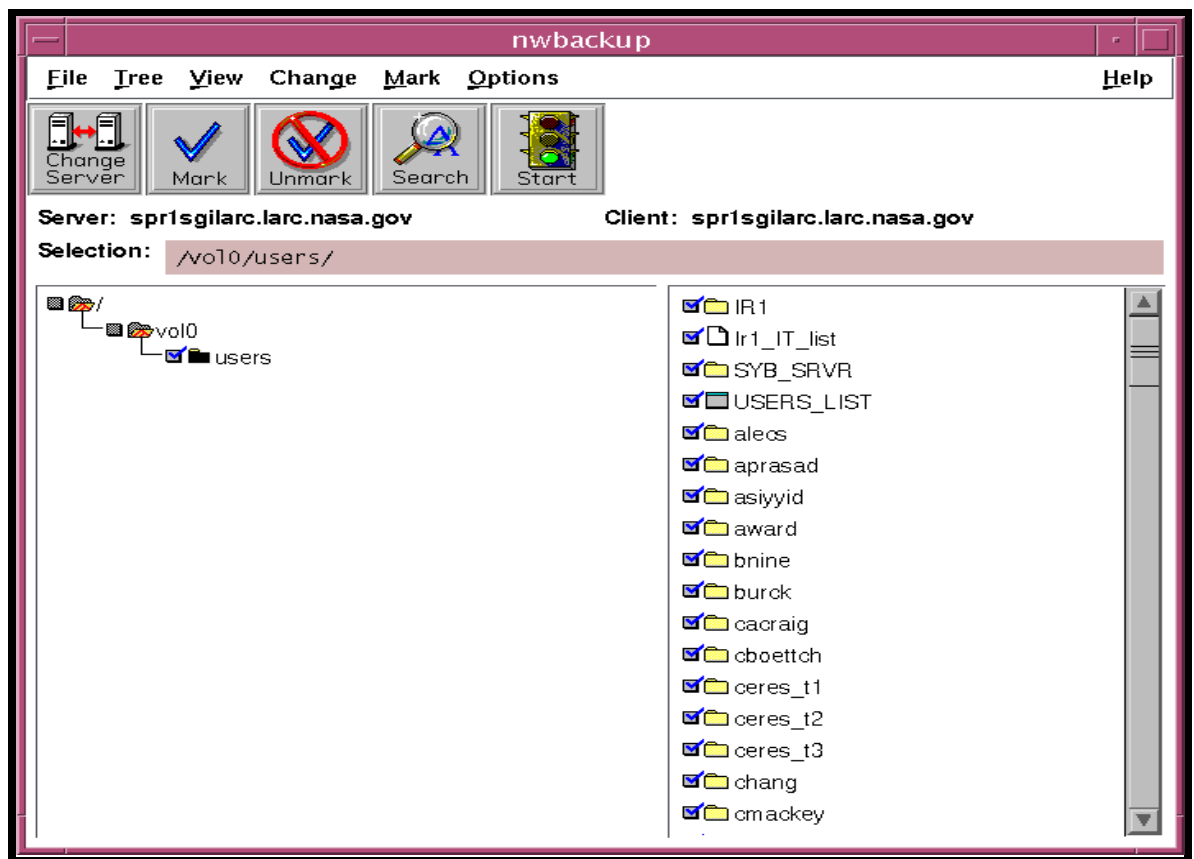


Figure 11. Networker Backup Window

- 8 If no **files/directories to be backed up** were provided by the requester, i.e. the whole machine is to be backed up, then type / in the **Selection** field and click the **Mark** button.
 - / is designated for backup and has a check next to it.
 - 9 If **files/directories to be backed up** were provided then select the **files/directories to be backed up** in the directory display and click the **Mark** button.
 - Drag scroll bar with mouse to scroll the list up and down.
 - Double click on directory name or the icon to list its contents.
 - To move up a directory level, type the path in the **Selection** field.
 - Clicking the **Mark** button or the square next to the file or directory name places a check mark (✓) in the box next to the name and designates the file for backup. If the file is a directory, all files under that directory are automatically marked.
 - 10 Click the **Start** button.
 - A **Backup Options** window opens.
 - 11 Click the **OK** button.
 - The **Backup Options** window closes.
 - The **Backup Status** window opens providing updates on the backup's progress.
 - 12 After the **Backup Completion Time** message appears in the **Backup Status** window, click the **Cancel** button.
 - The **Backup Status** window closes.
 - The backup is complete.
 - 13 Select **Exit** from the **File** menu to quit the Networker Backup program.
 - The Networker Backup window closes.
 - 14 At the UNIX prompt for the **machine to be backed up**, type **exit**, then press **Return**.
 - Root is logged out.
 - 15 Type **exit** again, then press **Return**.
 - You are logged out and disconnected from the machine to be backed up.
-

Single or Multiple File Restore

From time to time individual files or groups of files (but not all files) will have to be restored from an incremental backup tape due to operator error or system failure.

In order to perform the procedure, the System Administrator must have obtained the following information from the requester:

- Name of machine to be restored.
- Name of file(s) to be restored.
- Date from which to restore.
- User ID of the owner of the file(s) to be restored.
- Choice of action to take when conflicts occur. Choices are:
 - ☐ rename current file.
 - ☐ keep current file.
 - ☐ write over current file with recovered file.

Single or Multiple File Restore Procedure

- 1** Log into the **machine to be restored** by typing: **telnet *MachineRestored*** or **rsh *MachineRestored***, then press **Return**.
- 2** If a **Login:** prompt appears, log in as yourself by typing: ***YourUserID***, then press **Return**.
 - A password prompt is displayed.
- 3** Enter ***YourPassword***, then press **Return**.
 - Remember that ***YourPassword*** is case sensitive.
 - You are authenticated as yourself and returned to the UNIX prompt.
- 4** Log in as root by typing: **su**, then press **Return**. A password prompt is displayed.
- 5** Enter the ***RootPassword***, then press **Return**.
 - Remember that ***RootPassword*** is case sensitive.
 - You are authenticated as yourself and returned to the UNIX prompt.
- 6** Log in as the user by typing: **su *User'sID***.
 - You are authenticated as the **owner of the file(s) to be restored**.
- 7** Set display to current terminal by typing: **setenv DISPLAY *IPNumber:0.0*** or **setenv DISPLAY *MachineRestored:0.0***, then press **Return**.
- 8** Execute the Networker Recovery program by entering: **nwrecover**, then press **Return**.
 - A window opens for the **Networker Recovery** program (Figure 12). You are now able to perform restores of files.

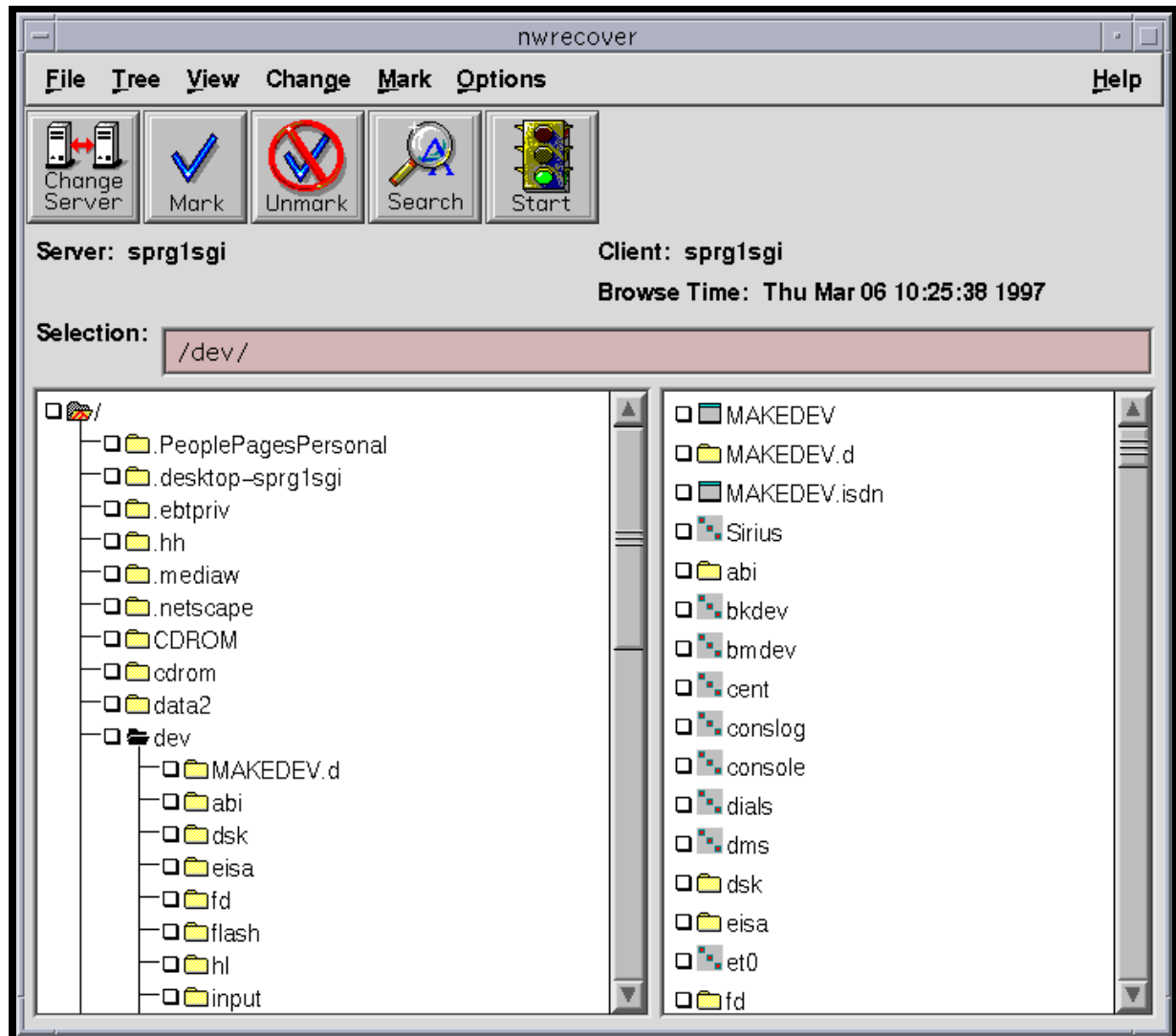


Figure 12. Networker Recovery Window

- 9 Select **file(s) to be restored** and click the **Mark** button.
 - Drag scroll bar with mouse to scroll the list up and down.
 - Double click on directory name to list its contents.
 - Clicking the **Mark** button or the square next to the file or directory name places a check mark (✓) in the box next to the name and designates the file for backup. If the file is a directory, all files under that directory are automatically marked.
- 10 Go to the **Change** menu, select **Browse Time**.
 - The **Change Browse Time** window opens.

- 11 Select the **date from which to restore**.
- NetWorker will automatically go to that day's or a previous day's backup which contains the file.
- 12 Click the **Start** button.
- The **Conflict Resolution** window opens ().

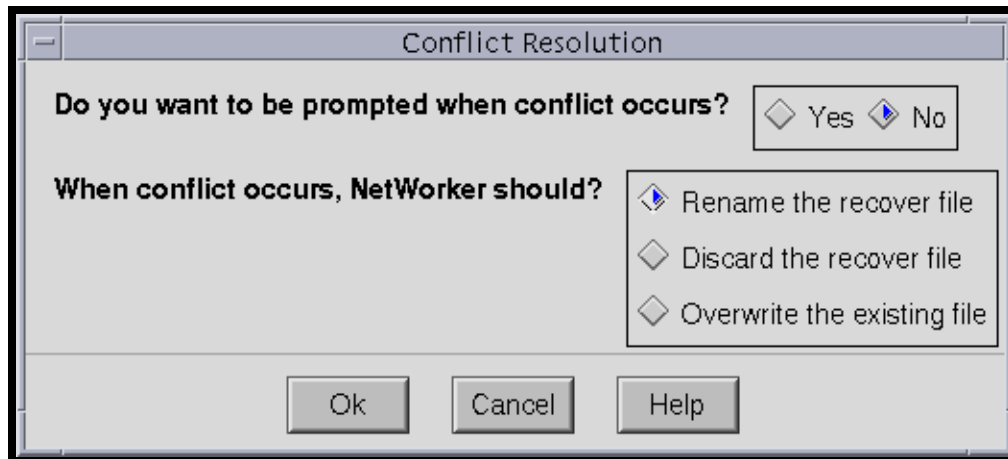


Figure 13. Conflict Resolution window.

- 13 Answer "Do you want to be prompted when conflicts occurs" by clicking the **yes** button, then click the **OK** button.
- When prompted with a conflict, choices of action are:
 - Rename the recover file, in which the filename on disk remains the same and the filename that comes from the tape will is named **filename.R**.
 - Discard the recover file, in which the file coming from the tape is not written to the disk.
 - Overwrite the existing file, in which the file coming from the tape overwrites the file on the disk.
 - Select the requester's **choice of action to take when conflicts occur**.
 - The **Recover Status** window opens providing information about the file restore.
 - If the required tapes are not in the drive, a notice will appear.
 - Click the **OK** button in the notice window.
 - If prompted for tapes, click **Cancel** in the **Recover Status** window and execute the Index Tapes procedure.
- 14 When a **recovery complete** message appears, click the **Cancel** button.

- 15 Go to the **File** menu, select **Exit**.
 - The Networker Recovery program quits.
 - 16 Type **exit**, then press **Return**.
 - The **owner of the file(s) to be restored** is logged out.
 - 17 Type **exit** again, then press **Return**.
 - Root is logged out
 - 18 Type **exit** one last time, then press **Return**.
 - You are logged out and disconnected from the **machine to be restored**.
-

Complete System Restore

A complete system restore is an emergency procedure that should be performed only in the event of a system crash with the loss of data and the only way to get the system back up and running in a timely fashion is to restore the system from a previous backup. The result of this action will be that any updates to the system between the last backup and the time of the restore will be lost. The System Administrator will determine which complete backup tape(s) to use (Figure 14). Depending on the frequency of complete system backups and incremental backups, data loss can be minimized.

A complete system restore involves restoring a number of tapes depending upon the particular situation. For example, should a system failure occur immediately after a full system backup was performed, only the tapes used in that backup will be required to restore the system to its usable state. However, if there was a period of time between the last full system backup and the system failure, tapes from the last full system backup as well as partial and incremental backups will have to be restored. This may become a time consuming process depending on the server affected, how much data is to be recovered, and how many tapes need to be restored. Additionally, the System Administrator may determine that only one or two of the many partitions need to be restored to make the system whole again. Therefore, these procedures will have to be mixed and matched to determine the proper restoration procedure for a given situation.

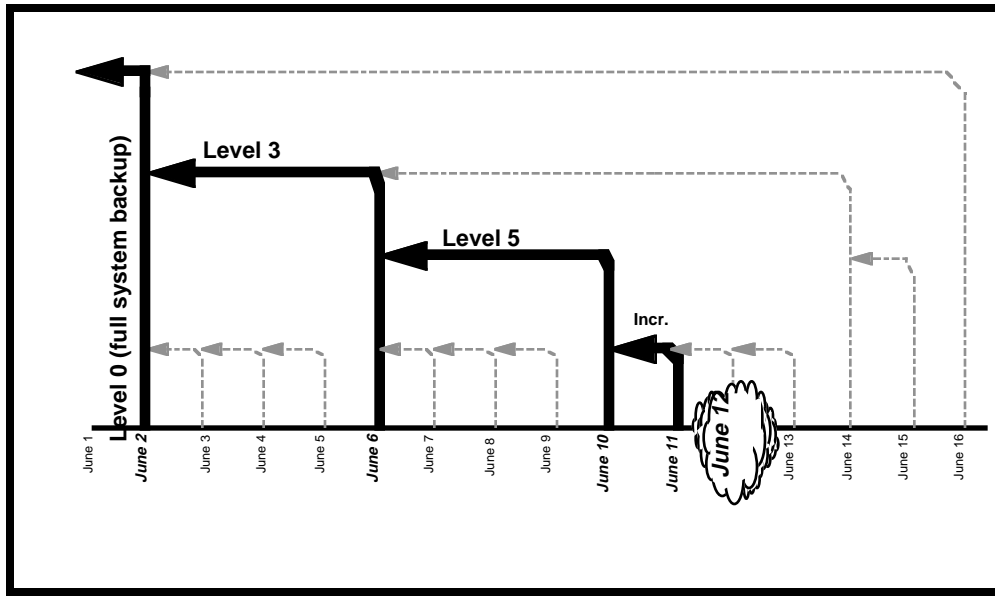


Figure 14. Tapes Required for Full System Restore.

In order to perform the procedure, the System Administrator must have obtained the following information about the requester:

- Name of system to be restored
- Date from which to restore

Full System Restore Procedure

- 1 Log into the backup server by typing: **telnet BackupServerName** or **rsh BackupServerName**, then press **Return**.
- 2 If a **Login:** prompt appears, log in as yourself by typing: **YourUserID**, then press **Return**.
 - A password prompt is displayed.
- 3 Enter **YourPassword**, then press **Return**.
 - Remember that **YourPassword** is case sensitive.
 - You are authenticated as yourself and returned to the UNIX prompt.
- 4 Log in as root by typing: **su**, then press **Return**.
 - A password prompt is displayed.
- 5 Enter the **RootPassword**, then press **Return**.

- Remember that *YourPassword* is case sensitive.
 - You are authenticated as yourself and returned to the UNIX prompt.
- 6 Set display to current terminal by typing: **setenv DISPLAY IPNumber:0.0** or **setenv DISPLAY BackupServerName:0.0**, then press **Return**.
 - 7 Execute the Networker Administrator program by entering: **nwadmin**, then press **Return**.
 - A window opens for the Networker Administrator program (Figure 15).
 - You are now able to perform restores of partitions.

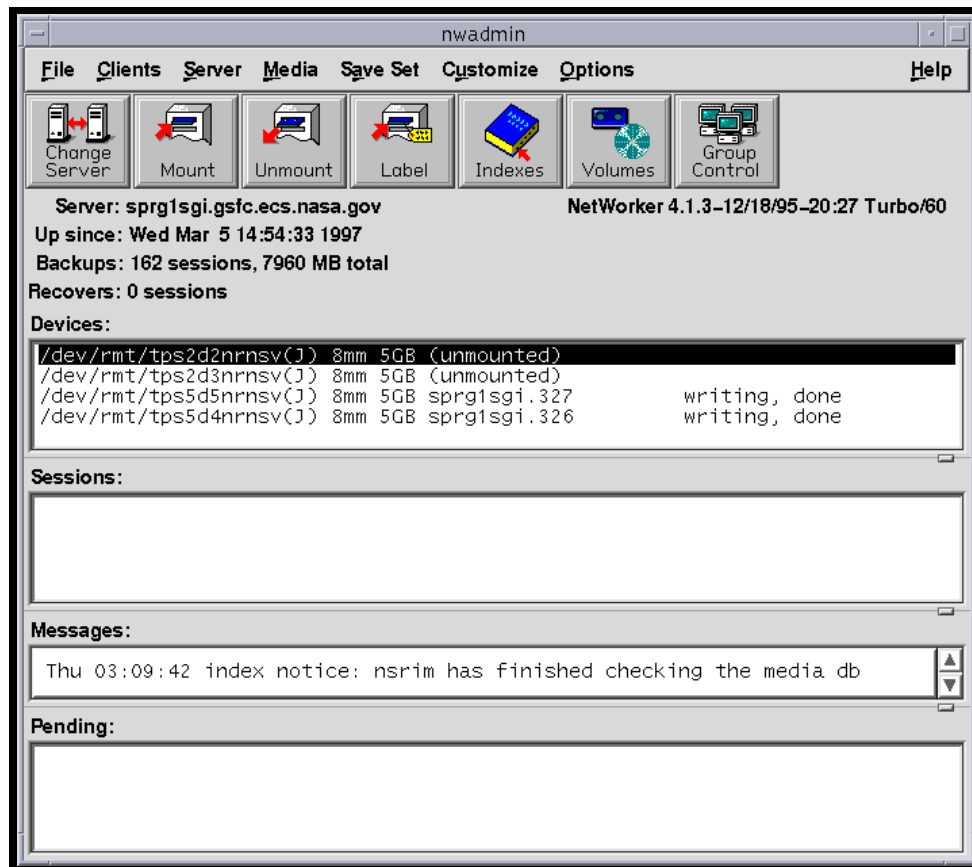


Figure 15. Networker Administrator's Window

- 1 Go to the **Save Set** menu, select **Recover Set**. The **Save Set Recover** window opens.
 - A **Save Set** is a pre-programmed set of Networker clients/servers, directories, and files that are included in a particular backup run.
- 2 Select the **Name of system to be restored** (referred to as **System** in the rest of this procedure) in the **Client** field's menu.

- The **Save Set** listing updates. This is a listing of partitions on the **System**.
 - At this time, note the partitions listed for the **System**. To do a complete system restore, this procedure needs to be performed for each partition listed.
- 3 Select the **Save Set**/partition from the listing.
- The **Instance** listing updates.
- 4 Select the appropriate **Instance**.
- An **Instance** is the date (and time) that a particular Save Set is run. A listing of **Instances** is a report detailing the Networker client backups that have occurred.
 - Select an **Instance** based upon the **Date from which to restore** (referred to as **Date** in the rest of this procedure) and of an appropriate level:
- Note 1:* To determine a base **Date**, you must consider the time of day that backups occur. For example, if the backup occurs at 02:00 each morning then a system corrupted at noon on June 6 would require a restoration of the June 6 backup. However, if the system corruption took place around the time of the backup, it would be more prudent to use the backup from June 5.
- If the backups are full or incremental, perform the following actions:
 - Select the most recent full backup that occurred on or prior to the **Date** and perform a partition restore. If the date of this full backup is not the same as the **Date**, perform a partition restore using each incremental backup, in chronological order, between this full backup and the day after the **Date**.
 - If the backups are of different numerical levels, follow these steps:
 - First select the most recent level 0/full backup prior to or on the **Date** and perform a restore of the partition. If a level 0/full backup did not occur on the **Date**, select the most recent backup of the next highest level occurring after this level 0 and prior to or on the **Date**. Perform a restore of the partition. Continue to select the most recent backup of the next highest level occurring between the last used **Instance** and the day after the **Date** until reaching an instance on the **Date**.
 - You can double click an **Instance** to see which tape is required.
- 5 Click the **Recover** button.
- The **Save Set Recover Status** window opens.
 - Clicking the **Volumes** button will show which tapes are required.
- 6 Click the **Options** button.
- The **Save Set Recover Options** window opens.
- 7 Set **Duplicate file resolution** to **Overwrite existing file** by clicking its radio button.
- 8 Make sure that the **Always prompt** checkbox is not checked.

- 9 Click the **OK** button.
 - The **Save Set Recover Options** window closes.
 - 10 Click the **Start** button in the **Save Set Recover Status** window.
 - Status messages appear in the **Status** box.
 - A **recovery complete** message appears when recovery is complete.
 - 11 Click the **Cancel** button after the **recovery complete** message appears.
 - The **Save Set Recover Status** window closes.
 - 12 If additional partition restores are required, go to step 8. Otherwise, select **Exit** from the **File** menu to quit the Networker Administrator program.
 - 13 At the UNIX prompt for the backup server, type **exit**, then press **Return**.
 - 14 Type **exit** again, then press **Return**.
-

System Logs

Logs are used to track events on the system. An *event* is the success or failure of an action. By reading and maintaining logs, system administrators can troubleshoot problems.

Some logs, such as **syslog**, **cronlog**, and **sulog**, are automatically maintained by the UNIX system. Other logs are created by specific applications, whether they are COTS or custom packages. The files are ASCII text files and that track system activity (syslog), cron schedule activity (cronlog) and who is using the super-user password (sulog).

Paths to the various log files vary from system to system, and therefore you must be aware of where these files are.

The UNIX system normally checks size thresholds and either truncates the log or copies the file to a backup (syslog to osyslog) when a threshold is reached.

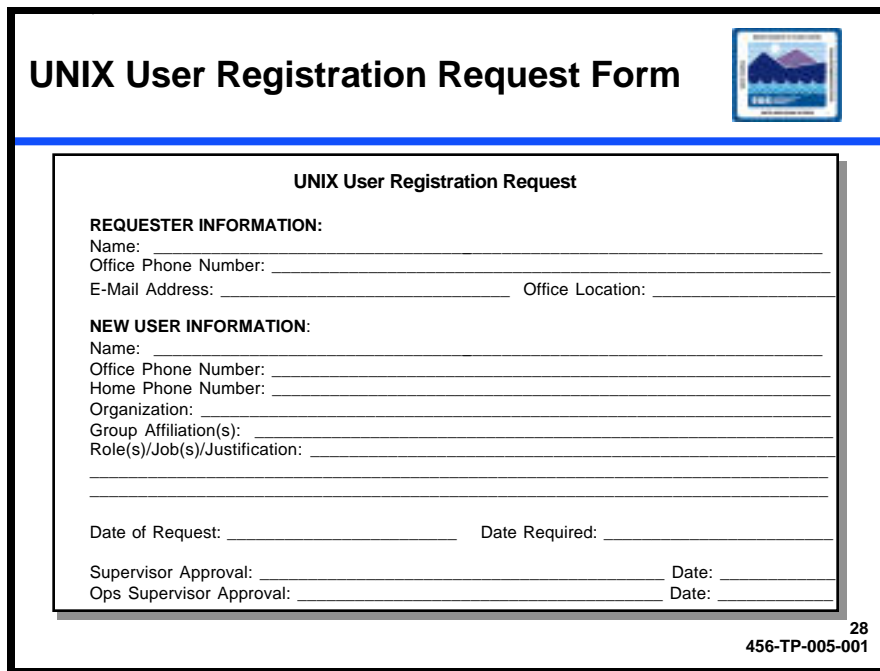
This page intentionally left blank.

User Administration

Add a New User

Adding a user to the system is accomplished through a series of steps that may be performed as a suite from the command line, or by use of a script. The procedure below outlines the individual steps that are required to completely set up a new user on the system. The script, if and when it is available, will accomplish these steps in an interactive manner.

The requester fills out a "User Registration Request Form" (Figure 16) and submits it to the supervisor. The requester's supervisor reviews the request, and if s/he determines that it is appropriate for the requester to have an account, forwards the request to the System Administrator. The System Administrator verifies that all required information is contained on the form. If it is, s/he forwards the request to the approval authority; the DAAC Manager. Incomplete forms are returned to the requester's supervisor for additional information. If the request for the accounts fits within policy guidelines, the DAAC Manager approves the request and returns the request form to the System Administrator to implement.



The image shows a form titled "UNIX User Registration Request Form". The form is enclosed in a black border. At the top right of the form is a small logo. The form itself has a white background with a blue border. The title "UNIX User Registration Request Form" is at the top left of the form. Below the title is a section titled "REQUESTER INFORMATION:" with fields for Name, Office Phone Number, E-Mail Address, and Office Location. Below that is a section titled "NEW USER INFORMATION:" with fields for Name, Office Phone Number, Home Phone Number, Organization, Group Affiliation(s), and Role(s)/Job(s)/Justification. At the bottom of the form are fields for Date of Request, Date Required, Supervisor Approval, and Ops Supervisor Approval. The form number "456-TP-005-001" and the page number "28" are at the bottom right of the form.

UNIX User Registration Request Form

UNIX User Registration Request

REQUESTER INFORMATION:
Name: _____
Office Phone Number: _____
E-Mail Address: _____ Office Location: _____

NEW USER INFORMATION:
Name: _____
Office Phone Number: _____
Home Phone Number: _____
Organization: _____
Group Affiliation(s): _____
Role(s)/Job(s)/Justification: _____

Date of Request: _____ Date Required: _____

Supervisor Approval: _____ Date: _____
Ops Supervisor Approval: _____ Date: _____

28
456-TP-005-001

Figure 16. User Registration Request Form

The System Administrator should be familiar with a UNIX text editor and the files **/etc/passwd.y** (Figure 17), **/etc/group** (Figure 18), and **/etc/auto.home** (Figure 19).

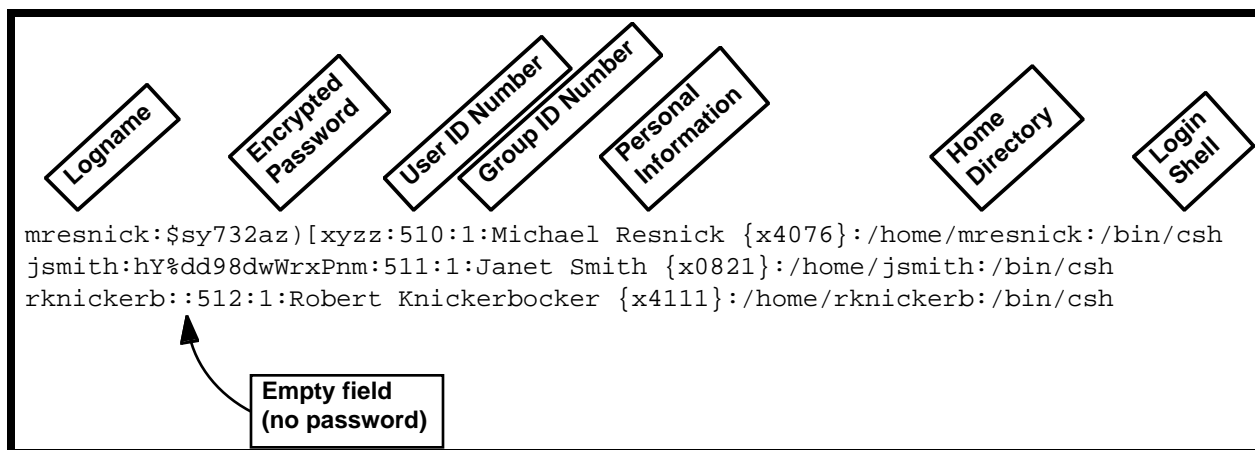


Figure 17. `/etc/passwd` File Fields

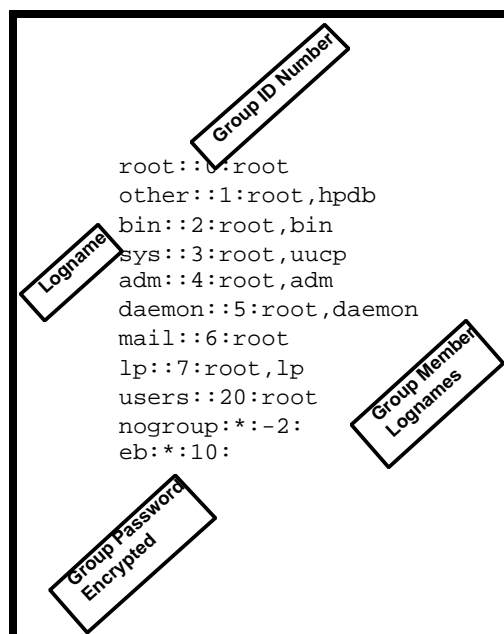


Figure 18. `/etc/group` File

Logname	Permissions	Location of Home Directory
dwashing	-rw,intr	acmnlsgi:/vol0/users/dwashing
jmangum	-rw,intr	acmnlsgi:/vol0/users/jmangum
mlynch	-rw,intr	acmnlsgi:/vol0/users/mlynch
ddavis	-rw,intr	acmnlsgi:/vol0/users/ddavis
rcampbel	-rw,intr	acmnlsgi:/vol0/users/rcampbel
spete	-rw,intr	acmnlsgi:/vol0/users/spete
kkleis	-rw,intr	acmnlsgi:/vol0/users/kkleis
echeung	-rw,intr	acmnlsgi:/vol0/users/echeung

Figure 19. /etc/auto.home File

Add a New User Procedure

*NOTE: These steps are the components that are included in the shell program /vol0/admin/exec/newuser. To run this script properly, you must be logged on to the NIS Master Server as **root**. Should the script not be available, you will need to perform each of these steps in order.*

- 1** Log onto the NIS Master server as **root** and enter the appropriate password at the **Password:** prompt.
- 2** Change to the /etc directory by typing at the UNIX prompt, **cd /etc**, then press **Return**.
- 3** Make a backup of the **passwd.yp** file by typing at the UNIX prompt, **cp passwd.yp passwd.yp_mmddyy**, where **mmddyy** is the current month, day and year. Then press **Return**.
- 4** Using the text editor of your choice, open the **passwd.yp** file for editing.
- 5** Copy the last line of the file and place it at the end of the file.
- 6** Make appropriate changes to the following fields which are delimited by colons (:):
 - **logname** – when possible, the logname consists of the user’s first name initial plus up to the first seven characters of the user’s last name for a maximum of eight characters; e.g., Janet Smith = jsmith; Robert Knickerbocker = rknickebr.
 - **password** – the encrypted password that was copied from the preceding line should be erased. There should be adjacent colons (::) in that location.
 - **user ID** – the User ID is a unique number, usually the next number in sequence. Check through the file to be sure the number you are planning to use is not already in use.

- **group ID** – the Group ID is a number that matches the group name from the **/etc/group** file. If a new group is to be added, it must be added to the **/etc/group** file before the user is officially added to the system.
 - **user's name and other information** – the user's real name, office location, telephone number, and any other information the System Administrator deems appropriate may be placed in this field. Do not use colons within the field to separate data.
 - **home directory** – the user's home directory will always be in the **/home** directory and be named the same as the user's logname; e.g., Janet Smith's home directory will be **/home/jsmith**; Robert Knickerbocker's home directory will be **/home/rknickerb**.
 - **default shell** – the default shell will be **/bin/csh**.
- 7 When all change have been made, save the file.
 - 8 Using the text editor of your choice, open the **/etc/auto.home** file for editing.
 - 9 Copy the last line of the file and place it at the end of the file.
 - 10 Make appropriate changes to the following fields which are delimited by colons (:):
 - **logname** – the logname should be the same as the logname used in the **/etc/passwd** file.
 - **mount point** – the mount point is always **/vol0/users/logname**.
 - 11 When all changes have been made, save the file.
 - 12 Create the user's new home directory by typing at the UNIX prompt: **mkdir /vol0/users/logname**, then press **Return**.
 - 13 At the UNIX prompt, type **cd /var/yp**, then press **Return**.
 - This changes your current directory to the **/var/yp** directory.
 - 14 At the UNIX prompt, type **./ypmake passwd auto.home**, then press **Return**.
 - This “pushes” the **passwd** and **auto.home** files out to all the network servers.
 - 15 Copy the administrative dot files to the new home directory by typing at the UNIX prompt: **cp /vol0/users/dotfiles/DAACTName /vol0/users/logname**, then press **Return**.
 - The administrative dot files include but are not limited to: **.Owdefaults**, **.Xauthority**, **.Xdefaults**, **.ab_library**, **.cshrc**, **.desksetdefaults**, **.login**, **.mwmrc**, **.openwin-init**, **.sh_history**, and **.xinitrc**.
 - 16 Change to the new home directory by typing at the UNIX prompt: **cd /vol0/users/logname**, then press **Return**.
 - 17 Change the permissions on all files to Read, Write, and Execute for owner and group, and Read and Execute for others by typing at the UNIX prompt: **chmod -R 775 /vol0/users/logname**, then press **Return**.

- 18 Change the ownership of all files by typing at the UNIX prompt: **chown -R logname /vol0/users/logname**, then press **Return**.
 - 19 Change the group of all files by typing at the UNIX prompt: **chgrp -R groupname /vol0/users/logname**, then press **Return**.
 - The default *groupname* is **user**.
 - 20 Check to ensure that all settings have taken place by typing at the UNIX prompt: **ls -la**, then press **Return**.
-

After the user is registered, the user is instructed to change his/her password if local DAAC policy requires. See **Changing a User's Password** for further instructions.

Deleting a User

A user's account is never completely deleted from the system. Essentially, the System Administrator should simply disable the user's password, backup the user's files to tape or disk according to DAAC policy, and then remove the user's home directory from the system.

Delete User Procedure

- 1 Log onto the NIS Master server as **root** and enter the appropriate password at the **Password:** prompt.
- 2 Change to the **/etc** directory by typing at the UNIX prompt, **cd /etc**, then press **Return**.
- 3 Make a backup of the **passwd.yp** file by typing at the UNIX prompt, **cp passwd.yp passwd.yp_mmddyy**, where *mmddyy* is the current month, day and year. Then press **Return**.
- 4 Using the text editor of your choice, open the **passwd.yp** file for editing.
- 5 Locate the line corresponding to the user you intend to delete from the system.
- 6 Position the cursor on the first character of the encrypted password field and delete all characters up to but not including the next colon.
- 7 In the position that the encrypted password used to be, type **DISABLED**.
- 8 When all changes have been made, save the file.
- 9 At the UNIX prompt, type **cd /var/yp**, then press **Return**.
 - This changes your current directory to the **/var/yp** directory.
- 10 At the UNIX prompt, type **./ypmake passwd**, then press **Return**.
 - This "pushes" the **passwd** file out to all the network servers.

- 11 At the UNIX prompt, type **cd /vol0/users/Logname**, then press **Return**.
 - This places you in the user's home directory.
 - 12 At the UNIX prompt, type **mkdir /tmp/Logname**.
 - This creates a sub-directory that will hold all of *Logname*'s files.
 - 13 At the UNIX prompt, type **find . -user Logname -print | cpio -pdmv /tmp/Logname**, then press **Return**.
 - This locates all files owned by *Logname* and copies them to the /tmp directory.
 - 14 Perform a backup of the files in the /tmp/Logname directory either immediately or during the next round of backups.
 - 15 If space is needed, remove the user's home directory and all files from the system:
 - At the UNIX prompt, type **find / -user Logname -print -exec rm {} \;**, then press **Return**.
 - At the UNIX prompt, type **find / -user Logname -type d -exec rmdir {} \;**, then press **Return**.
 - This last step may have to be repeated several times to remove all of the user's subdirectories.
-

Changing a User's Password

The System Administrator may be called upon to change a user's password when a user verifies that he/she has forgotten the password. Should the user forget the password, the System Administrator will reassign that user's password and force the user to change it immediately upon logging in.

Change User Password Procedure

- 1 Log into the NIS Master Server as **root**.
- 2 At the UNIX prompt, type **yppasswd Logname**, then press **Return**.
 - The system responds with **Changing NIS password for Logname...**
- 3 At the **Old NIS password:** prompt, type the old password, then press **Return**.
- 4 At the **New Password:** prompt, type the new password, then press **Return**.
 - Passwords are six to eight characters in length and must include at least one non-alphabetic character
 - Numbers, spaces, and special characters are acceptable.
 - Uppercase and lowercase letters are considered unique.

5 At the **Retype new password:** prompt, type the new password again, then press **Return**.

- If the new password and re-entered new password do not match, the password is not changed.
 - If the new password and the retyped password do match, the password is changed and the system responds with **The NIS passwd has been changed on enterprise, the master NIS passwd server.**
-

Checking File Access Permission

File access permissions are assigned to every file and directory created on the system at the time it is created. The system's **umask** is set by the System Administrator to determine the permission levels allowed.

Whenever a long directory listing is requested, the file access permissions are displayed along with a host of additional information described in the procedure below.

Checking File/Directory Access Privileges Procedure

1 At a UNIX prompt, type **cd *Path***, press **Return**.

- The ***Path*** is the full path up to but not including the file/directory on which access privilege status is needed. For example, if the requester wants access privileges status on directory `/home/jdoe`, then type **cd /home** and press **Return**.

2 From the UNIX prompt, type **ls -la**. The output from the command should appear as below:

drwxrwxrwx	3	mresnick	training	8192	Jun 14 08:34	archive
drwxr-xr-x	11	mresnick	training	4096	Jul 03 12:42	daacdata
-rw-rw-rw-	1	mresnick	training	251	Jan 02 1996	garbage
lrw-r--r--	2	jjones	admin	15237	Apr 30 20:07	junk
-rwxr--rw-	1	mresnick	training	5103	Oct 22 1994	trash

- The first column of output is the file access permission level for the file (see Figure 20 below for a description of file permissions).
- The next column to the right is the number of links to other files or directories.
- The third column is the file owner's user ID
- The fourth column is the group membership of that owner.
- The fifth column shows file size in bytes.
- The sixth column displays the date and time of last modification (if the date is more than six months old, the time changes to the year)

- The last column displays the file name.

Changing a File/Directory Access Permission

File and directory access privileges are displayed in the first output column of the **ls -l** command and consists of ten characters, known as **bits**. Each bit refers to a specific permission. The permissions are divided into four groupings shown and briefly described in Figure 20:

		OWNER permissions			GROUP permissions			OTHER permissions		
	d	r	w	x	r	w	x	r	w	x
	l	r	w	-	r	w	-	r	w	-
	-	r	w	x	r	-	x	r	w	x
	-	r	w	-	r	-	-	r	-	-

d=directory, l=file

r= read	<i>Look/copy/print</i>
w= write	<i>Change/save/delete</i>
x= execute	<i>Run commands/ use directory</i>

Figure 20. Access permissions

Each READ permission is worth 4 points. Each WRITE permission is worth 2 points. Each EXECUTE permission is worth 1 point. Denying permission (a dash in the permission's position) is worth 0 points.

To determine the permission level, or **mode** of a file, add the points for each user category to come up with a three-digit number (e.g., 755).

Next, determine what the new mode will look like visually. For example, the first file in the above figure currently shows a mode of **rw-rw-rw-**. The new mode will be **rw-r-x---**.

Now, translate the new mode into the three-digit number (750). Now you can perform the procedure below.

In order to perform the procedure, the System Administrator must have obtained the following information about the requester:

- full path of the file/directory on which access privileges will be changed.
- new access privileges to set on the file/directory. Can be any of:
 - ☐ New owner
 - ☐ New group
 - ☐ New user/owner privileges (read, write and/or execute)
 - ☐ New group privileges (read, write and/or execute)
 - ☐ New other privileges (read, write and/or execute)

Changing a File/Directory Access Privilege Procedure

- 1 At the UNIX prompt, type **su**, press **Return**.
- 2 At the **Password** prompt, type **RootPassword**, press **Return**.
 - Remember that **RootPassword** is case sensitive.
 - You are authenticated as root.
- 3 Type **cd Path**, press **Return**.
 - The **Path** is the full path up to but not including the file/directory on which access privileges will be changed. For example, if the requester wants access privileges changed on directory /home/jdoe then type **cd /home** and press **Return**.
- 4 If there is a **New owner** then type **chown NewOwner Filename(s)**, press **Return**.
 - The **Filename(s)** is the name of the file or directory on which access privileges will be changed. For example, if the requester, whose logname is **psmith**, wants access privileges changed on directory /home/jdoe then type **chown psmith /home/jdoe** and press **Return**.
- 5 If there is a **New group** then type **chgrp NewGroup Filename(s)**, press **Return**.
 - The **Filename(s)** is the name of the file or directory on which access privileges will be changed. For example, if the requester, whose group is **users**, wants access privileges changed on directory /home/jdoe then type **chgrp users /home/jdoe** and press **Return**.
- 6 If there are new user, group, or other privileges:
 - Determine the current mode of the file.
 - Determine the new mode of the file

- At the UNIX prompt, type **chmod *NewMode Filename(s)***, then press **Return**.
- 7 Type **exit**, press **Return**.
- Root is logged out.
-

Moving a User's Home Directory

The Moving a User's Home Directory process begins when the requester submits a request to the Ops Supervisor. The Ops Supervisor approves or denies the request. Once approved, the request is forwarded to the SA who moves the user's home directory. When the changes are complete the SA notifies the requester and Ops Supervisor.

Moving Home Directory Procedures

If the directory name is to be changed:

- 1 At the UNIX prompt, type **mv *OldDirName NewDirName***, then press **Return**.

If the directory is to be moved to another file system:

- 1 At the UNIX prompt, type **cd /vol0/users**, then press **Return**.
- 2 At the UNIX prompt, type **find *Logname* -print | cpio -pdmv *NewFSName***, then press **Return**.
 - This locates all the files from the original directory and reconstructs the file structure in the new location.
- 3 Change to the /etc directory by typing at the UNIX prompt, **cd /etc**, then press **Return**.
- 4 Make a backup of the **passwd.yp** file by typing at the UNIX prompt, **cp passwd.yp passwd.yp_*mmddyy***, where ***mmddyy*** is the current month, day and year. Then press **Return**.
- 5 Using the text editor of your choice, open the **passwd.yp** file for editing.
- 6 Locate the line containing the user whose home directory you are changing.
- 7 Change the home directory field to reflect the new home directory of the user.
- 8 Save the file.
- 9 Using the text editor of your choice, open the **auto.home** file for editing.
- 10 Locate the line containing the user whose home directory you are changing.
- 11 Change the home directory field to reflect the new home directory of the user.
- 12 Save the file.

- 13** At the UNIX prompt, type **/var/ypmake passwd auto.home**, then press **Return**.
- This pushes the password and auto.home files out to the entire system.
- 14** After confirming that the files have been properly transferred, at the UNIX prompt type **rm -r *Logname***, then press **Return**.
- This removes the original home directory.
-

This page intentionally left blank.

New Workstation Installation

This section is included for the unlikely event that new workstations will need to be added during Pre-Release B Testbed implementation.

Installing a new workstation has three stages. Each stage has several sub-tasks that must be performed in a prescribed order. These steps include:

- Preparation
 - Preparing the hardware
 - Configuring the network
- Installation
 - Installing the hardware
 - Installing the operating system(s)
 - Installing the custom software
 - Installing the COTS software
- Testing and Verification
 - Rebooting the workstation
 - Logging onto the workstation

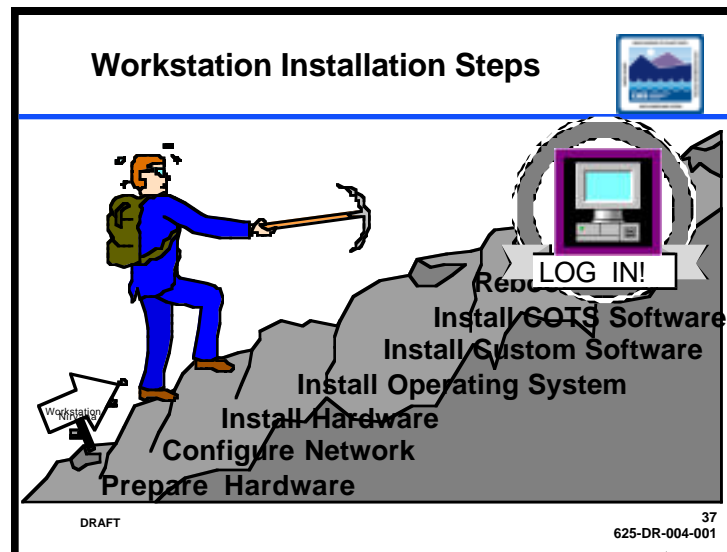


Figure 21. Workstation Installation Steps

Preparation

Hardware Preparation

The Hardware Preparation process begins when the requester submits a request to the System Administrator. The System Administrator then determines if the requested hardware is on hand or must be ordered. Once the hardware is available along with all the necessary attachments, the System Administrator will schedule the installation.

The System Administrator must obtain the following information from the requester:

- type of hardware desired (HP, Sun, SGI or NCD).
- location of installation.

Network Configuration

In a nutshell, all network configuration entails is giving the hardware device a name in accordance with the DAAC standard, and forwarding that information to the Network Monitor for assignment of an IP address and its addition to the network domain name service (DNS).

Network Configuration Procedure

- 1 Determine the name of the hardware.
 - Each hardware device is given name based on its local function, DAAC location and subsystem, brand, and sequential introduction into the system.
 - For example, the first SGI Science Processor file server at NSIDC would be named **sprn1sgi** (**spr**=Science Processor, **n**=NSIDC, **1**=first processor, **sgi**=brand).
 - For example, the third HP laser printer on the ASTER Sybase server at LaRC would be named **astl3hp** (**ast**=ASTER, **l**=LaRC, **3**=third printer, **hp**=brand).
 - 2 Submit a request to the Network Administrator for the IP address and the DNS entry.
-

Installation

Hardware

The actual installation of the hardware involves the logical steps of:

- removing the hardware from its packaging
- placing the hardware in the location prescribed in the Release A Installation Plan (800-TP-005-001)
- connecting the appropriate cables and wires

When these steps are completed in accordance with the procedures in the Release A Installation Plan (800-TP-005-001), the item(s) must be reported to inventory.

Reporting to Inventory Procedure

- 1 Locate the Inventory Control Number on each hardware component and record them. The Inventory Control Number is on a small bright sticker on the front of each hardware component.
 - 2 Submit the Inventory Control Numbers and location of the machine to the Inventory Controller.
-

Operating System Installation

*NOTE: Throughout this section, reference is made to a **download disk**. A download disk is a removable disk drive that is connected to the hardware device onto which software is to be installed.*

Solaris 2.4 Operating System Installation

Solaris 2.4 is also known as Sun OS 2.4. The Solaris 2.4 Operating System Installation process begins when the installation of hardware procedures have been completed.

This section explains how to install the Solaris 2.4 operating system, including network configuration and patch installation. If you would like a listing of the patches installed, please see document number 420-TD-012-001 Release A Sun Solaris Operating System Patch List.

Solaris 2.4 Operating System Installation Procedure

- 1 Get the download disk.
- 2 Check that it is set to be target 2.
 - The target number is found on the bottom of the disk.
 - You can change the target number by hitting the buttons above and below it.
- 3 Plug the download disk into the Sun
- 4 Power on the download disk.
 - Facing the front of the disk, the power switch is found on the back to the left of the disk.
- 5 Power on the monitor; power on the Sun.
 - When facing the front of the Sun, the power switch is located on the back right.
- 6 At the > prompt, type **probe-scsi**, then press **Return**.

- Verify that target 2 exists by finding it in the listing that appears. It will appear as **SCSI Disk: scsi(0)disk(2)**.
- 7 Type **boot disk2 -swr**, then press **Return**.
- The Sun boots up.
 - s is for single user; w is for writeable, and r is for reconfigure (required because you added a drive).
- 8 Type **RootPassword**, press **Return**.
- **RootPassword** is the root password for the download disk.
 - Remember that the **RootPassword** is case sensitive.
 - You are authenticated as root and returned to a UNIX prompt.
- 9 Type **/download/setup**, press **Return**.
- Status messages will be displayed.
- 10 When prompted for the Sun's name, type **SunsName**, press **Return**.
- 11 When prompted for the Sun's IP address, type **SunsIP**, press **Return**.
- The Sun's network and hostname are configured.
- 12 When you are returned to a UNIX prompt, type **/etc/halt**, press **Return**.
- 13 At the **>** prompt, power off the download disk.
- 14 Disconnect the download disk from the Sun.
- 15 At the **>** prompt, type **boot -r**, press **Return**.
- The Sun boots up.
 - r is for reconfigure (required because you removed a drive).
- 16 At the **login:** prompt, type **root**, press **Return**.
- 17 Type **RootPassword**, press **Return**.
- **RootPassword** is the root password for the download disk. (The Sun uses the download disk's root password until a new one is set.)
 - Remember that the **RootPassword** is case sensitive.
 - You are authenticated as root and returned the UNIX prompt.
- 18 Type **passwd root**, press **Return**.
- 19 At the **New password:** prompt, type **RootPassword**, press **Return**.
- **RootPassword** is the root password for the Sun.

- Remember that the **RootPassword** is case sensitive.
- 20** At the **Re-enter new password:** prompt, type **RootPassword**, press **Return**.
- **RootPassword** is the root password for the Sun.
 - This step confirms that the root password has been entered correctly.
 - Remember that the **RootPassword** is case sensitive.
 - The root password for this Sun is set. Inform all authorized personnel of **RootPassword**.
- 21** Type **exit**, press **Return**.
- Root is logged out of the SGI.
- 22** Inform the backup administrator of the new machine.
-

HP-UX 9.05 Operating System Installation

This section explains how to install the HP-UX 9.05 operating system, including network configuration and patch installation.

HP-UX 9.05 Operating System Installation Procedure

- 1** Get the download disk.
- 2** Check that it is set to be target 2.
 - The target number is found on the back of the disk.
 - You can change the target number by hitting the buttons above and below it.
- 3** Plug the download disk into the HP.
- 4** Power on the download disk.
 - The power switch is located on the back of the drive.
- 5** Power on the monitor, power on the HP.
 - The power switch is located on the right side of the HP, towards the front.
 - The HP starts booting up.
- 6** At the **Selecting a system to boot**. To stop selection process press and hold the **ESCAPE** key message, press and hold **Escape**.
 - You have 10 seconds to press **Escape** before the boot process proceeds.

- The boot process will stop and a menu of boot commands will appear.
- 7 Select boot scsi.2.0 by typing **b DeviceSelectionForscsi.2.0 isl**, press **Return**.
- For example, if the Device Selection for scsi.2.0 in the menu is P1 then type **b P1 isl** and then press **Return**.
 - **isl** will cause the HP to boot in interactive mode.
- 8 At the **ISL>** prompt, type **hpux -is boot disk(scsi.2;0)/hp-ux**, press **Return**.
- **-is** causes the HP to boot in single user mode.
 - You will be returned to the UNIX prompt.
- 9 Type **/download/setup**, press **Return**.
- Status messages will be displayed.
- 10 When prompted for the HP's name, type **HPsName**, press **Return**.
- 11 When prompted for the HP's IP address, type **HPsIP**, press **Return**.
- The HP's network and hostname are configured.
- 12 When you are returned to a UNIX prompt, type **/etc/shutdown -h -y now**, press **Return**.
- The HP shuts down and comes to a halt.
- 13 Once the HP has halted, power off the download disk, power off the monitor.
- 14 Power off the HP.
- 15 Disconnect the download disk from the HP.
- 16 Power on the monitor.
- 17 Power on the HP.
- The HP starts booting up.
- 18 At the **Selecting a system to boot. To stop selection process press and hold the ESCAPE key** message, press and hold **Escape**.
- You have 10 seconds to press **Escape** before the boot process proceeds.
 - The boot process will stop and a menu of boot commands will appear.
- 19 Select boot scsi.6.0 by typing **b DeviceSelectionForscsi.6.0**, press **Return**.
- For example, if the Device Selection for scsi.6.0 in the menu is P1 then type **b P1** and press **Return**.
- 20 At the **login:** prompt, type **root**, press **Return**.
- 21 Type **RootPassword**, press **Return**.

- ***RootPassword*** is the root password for the download disk. (The HP uses the download disk's root password until a new one is set.)
 - Remember that the ***RootPassword*** is case sensitive.
 - You are authenticated as root and returned the UNIX prompt.
- 22 Type **passwd root**, press **Return**.
- 23 At the **New password:** prompt, type ***RootPassword***, press **Return**.
- ***RootPassword*** is the root password for the HP.
 - Remember that the ***RootPassword*** is case sensitive.
- 24 At the **Re-enter new password:** prompt, type ***RootPassword***, press **Return**.
- ***RootPassword*** is the root password for the HP.
 - This step confirms that the root password has been entered correctly.
 - Remember that the ***RootPassword*** is case sensitive.
 - The root password for this HP is set. Inform all authorized personnel of ***RootPassword***.
- 25 Type **exit**, press **Return**.
- Root is logged out of the HP.
- 26 Inform the backup administrator of the new machine.
-

IRIX 5.3 and 6.2 Operating Systems Installation

This section explains how to install the IRIX 5.3 and 6.2 operating systems, including network configuration and patch installation. If you would like a listing of the patches installed for IRIX 5.3, please see document number 420-TD-013-001 Release A SGI IRIX 5.3 Operating System Patch.

IRIX 5.3 and 6.2 Operating Systems Installation Procedure

- 1 Get the download disk.
- 2 Check that it is set to be target 2.
 - The target number is found on the bottom of the disk.
 - You can change the target number by hitting the buttons above and below it.
- 3 Plug the download disk into the SGI.
- 4 Power on the download disk.
 - The power switch is located on the back of the drive.

- 5 Power on the monitor; power on the SGI.
 - The power switch is located on the front of the SGI, towards the left.
- 6 At the **Starting up the system...** message, click the **Stop for Maintenance** button.
 - You have only a few seconds to click the **Stop for Maintenance** button before the boot process proceeds.
 - The boot process will stop and a **System Maintenance** menu will appear.
- 7 Select **5 Enter Command Monitor**.
 - You will be returned to the Command Monitor prompt which is >>.
- 8 At the >> prompt, type **hinv**, press **Return**.
 - Verify that target 2 exists by finding it in the listing that appears. It will appear as **SCSI Disk: scsi(0)disk(2)**.
- 9 Type **boot -f dksc(0,2,0)sash**, press **Return**.
 - The SGI boots from the download disk into the stand alone shell.
 - You will be returned to a UNIX prompt.
- 10 Type **/download/setup**, press **Return**.
 - Status messages will be displayed.
- 11 When prompted for the SGI's name, type **SGIsName**, press **Return**.
- 12 When prompted for the SGI's IP address, type **SGIsIP**, press **Return**.
 - The SGI's network and hostname are configured.
- 13 When you are returned to a UNIX prompt, type **/etc/shutdown -y -g0**, press **Return**.
 - The SGI shuts down.
 - You will be returned to a >> prompt, a **System Maintenance** menu or a message saying that **this system can be powered off**.
- 14 Power off the download disk, power off the monitor.
- 15 Power off the SGI.
- 16 Disconnect the download disk from the SGI.
- 17 Power on the monitor.
- 18 Power on the SGI.
 - The SGI starts booting up.
- 19 At the **login:** prompt, type **root**, press **Return**.
- 20 Type **RootPassword**, press **Return**.

- **RootPassword** is the root password for the download disk. (The SGI uses the download disk's root password until a new one is set.)
 - Remember that the **RootPassword** is case sensitive.
 - You are authenticated as root and returned the UNIX prompt.
- 21** Type **passwd root**, press **Return**.
- 22** At the **New password:** prompt, type **RootPassword**, press **Return**.
- **RootPassword** is the root password for the SGI.
 - Remember that the **RootPassword** is case sensitive.
- 23** At the **Re-enter new password:** prompt, type **RootPassword**, press **Return**.
- **RootPassword** is the root password for the SGI.
 - This step confirms that the root password has been entered correctly.
 - Remember that the **RootPassword** is case sensitive.
 - The root password for this SGI is set. Inform all authorized personnel of **RootPassword**.
- 24** Type **exit**, press **Return**.
- Root is logged out of the SGI.
- 25** Inform the backup administrator of the new machine.
-

NCD Operating System Installation

This section explains how to configure the NCD, including putting the necessary start-up files in place on the server.

NCD Operating System Installation Procedure

- 1** Turn on the NCD and monitor. The monitor power button is on the lower front of the monitor. The NCD power switch is on the back, on the right.
 - The message **Boot Monitor Vx.x.x** will appear.
- 2** Press the **Escape** key twice.
 - You have only a few seconds to press the **Escape** key.
 - The boot process stops and a boot monitor prompt, **>**, appears.
 - If you do not see a **>** prompt then press the **Escape** key a few more times.
- 3** Press the **Setup** key.

- The **Main** menu will appear.
- 4 Go to the **Keyboard** menu by pressing the **Right Arrow** key.
 - The **Keyboard** menu appears.
- 5 Select **N-101** by pressing the **Down Arrow** key.
 - You may need to press the **Down Arrow** key a few times before **N-101** is selected.
- 6 Go to the **Monitor** menu by pressing the **Right Arrow** key.
 - The **Keyboard** menu disappears.
 - The **Monitor Resolution** menu appears.
- 7 Select **1600x1200 65 Hz** by pressing the **Down Arrow** key.
 - You may need to press the **Down Arrow** key a few times before **1600x1200 65 Hz** is selected.
- 8 Press the **Shift** and **T** keys.
 - This tests the new monitor resolution setting.
- 9 Use the + and - keys on the front of the monitor under the **ADJUST** label to adjust the screen.
- 10 Press the **STORE** key on the front of the monitor.
 - The monitor stores the screen adjustments.
- 11 Press the **Escape** key.
 - The monitor resolution test ends.
 - You are returned to the **Main** menu.
- 12 Go to the **Network** menu by pressing the **Right Arrow** key twice.
 - The **Monitor Resolution** menu disappears.
 - The **Network** menu appears.
- 13 Select **NVRAM** for the **Get IP Addresses From** option.
 - You can use the **Space Bar** to move between the available options.
- 14 Press the **Down Arrow** key.
- 15 Type the *NCDIPaddress* for the **Terminal IP Address** option, press the **Down Arrow** key.
 - The *NCDIPaddress* is in dotted decimal notation, for example, 155.157.21.34.
- 16 Type the *StartupFileServerIPaddress* for the **First Boot Host IP Address** option, press the **Down Arrow** key.

- The *StartupFileServerIPAddress* is in dotted decimal notation, for example, 155.157.44.22.
 - The *StartupFileServer* is the machine where the NCD startup files are stored.
- 17 Press the **Down Arrow** key twice.
- 18 Type the *NCDGatewayIPAddress* for the **Gateway IP address** option, press the **Down Arrow** key.
- The *NCDGatewayIPAddress* is in dotted decimal notation, for example, 155.157.44.22.
 - The *NCDGatewayIPAddress* is the same as the *NCDIPAddress* except the last number/octet is 1. For example, if the *NCDIPAddress* is 155.157.21.34, the *NCDGatewayIPAddress* is 155.157.21.1.
- 19 Press the **Down Arrow** key, type the *BroadcastIPAddress* for the **Broadcast IP Address** option.
- The *BroadcastIPAddress* is in dotted decimal notation, for example, 155.157.44.22.
 - The *BroadcastIPAddress* is the same as the *NCDIPAddress* except the last number/octet is 255. For example, if the *NCDIPAddress* is 155.157.21.34, the *BroadcastIPAddress* is 155.157.21.255.
- 20 Press the **Right Arrow** key.
- The **Network** menu disappears.
 - The **Boot** menu appears.
- 21 Type *Xncdhmx_s* for the **Boot File** option, press the **Down Arrow** key.
- 22 Press the **Down Arrow** key, type */data/ncd/* for the **NFS Boot Directory** option, press the **Down Arrow** key.
- 23 Press the **Down Arrow** key, type */usr/lib/X11/ncd/configs/* for the **UNIX Config Directory** option, press the **Down Arrow** key.
- 24 Press the **Down Arrow** key, press the **d** key. The **TFTP Order** option is set to **Disabled**.
- 25 Press the **Down Arrow** key, press the **1** key. The **NFS Order** option is set to **1**.
- 26 Press the **Down Arrow** key, press the **d** key. The **MOP Order** option is set to **Disabled**.
- 27 Press the **Down Arrow** key, press the **d** key. The **LOCAL Order** option is set to **Disabled**.
- 28 Press the **Right Arrow** key.
- The **Boot** menu disappears.
 - The **Done** menu appears. **Reboot** is selected.
- 29 Press the **Return** key.
- The NCD reboots.

- Status messages appear.
- 30 Log into the *StartupFileServer* by typing: **telnet *StartupFileServer*** or **rsh *StartupFileServer*** at a UNIX prompt, then press **Return**.
- 31 If a **Login:** prompt appears, log in as yourself by typing: *YourUserID*, then press **Return**. A password prompt is displayed.
- 32 Enter *YourPassword*, then press **Return**.
- Remember that *YourPassword* is case sensitive.
 - You are authenticated as yourself and returned to the UNIX prompt.
- 33 Log in as root by typing: **su**, then press **Return**.
- A password prompt is displayed.
- 34 Enter the *RootPassword*, then press **Return**. Remember that the *RootPassword* is case sensitive. You are authenticated as root and returned to the UNIX prompt.
- 35 Type **cd /usr/lib/X11/ncd/configs**, press **Return**.
- 36 Type **./i**, press **Return**.
- **i** is a script which builds a NCD startup file.
- 37 Type the last two numbers/octets of the *NCDIPAddress* when the script prompts you for the **IP address**, press **Return**. For example, if the *NCDIPAddress* is 155.157.21.34 then type **21.34** and then press **Return**.
- 38 Type the *NCDLoginHost* when the script prompts you for the **Login Host**, press **Return**.
- The *NCDLoginHost* is the name of one of the X-servers.
- 39 When the script prompts you for the **NCD Number**, type the *NCDname* minus the “ncd” part. For example, if the *NCDname* is ncd2 then the **NCD Number** is 2.
- Some status messages appear telling you what the script is doing.
 - The script exits.
- 40 Type **exit**, then press **Return**.
- Root is logged out
- 41 Type **exit** again, then press **Return**.
- You are logged out and disconnected from the *StartupFileServer*.
-

Software Installation

Custom and COTS software will be pre-installed on all Pre-Release B Testbed CIs. Copies of all software packages are stored in the /vol0/admin/exec directory in a compressed tar format in the unlikely event that the software will have to be restored to the system.

All software will be delivered via the shell program **deliver_tar.sh**. It is an interactive program that prompts you with questions regarding the name of the software package to deliver, the location of where it will be configured, and other questions.

This procedure assumes that following actions have already been taken:

- The upgrade has been previously scheduled and noted in the resource plan.
- The software package was obtained by FTP (File Transfer Protocol) and tar tapes including any associated install scripts/makefiles are in ClearCase at the site.
- The detailed steps for installation have been provided in the VDD accompanying the software package.
- The reconfiguration to minimize impact to existing operational resources has been defined.

Software Installation Procedure

- 1** Resource Manager composes an information message to the affected operators stating that the affected resources will be taken down as scheduled.
- 2** Resource Manager asks the Production Monitor to verify that the production has completed on the resource as planned.
- 3** Production Monitor checks current load on target resources and produces a display of the current jobs running on the requested production resources.
- 4** Production Monitor informs Resource Manager that production jobs are complete.
- 5** Resource Manager shuts down any processes still running on the impacted host(s).
- 6** Resource Manager begins shut down procedures to take host off-line.
- 7** Resource Manager, operators, and Sustaining Engineer receive a message from HP OpenView indicating that the desired host has gone off-line.
- 8** Resource Manager notifies Sustaining Engineer that the host is available for upgrade.
- 9** At the UNIX prompt, type **deliver_tar.sh**, then press **Return**.
- 10** Answer all questions asked and press **Return** at the end of each response.
- 11** Sustaining Engineer verifies that all of the paths and directory structures have been created and are correct.
- 12** Sustaining Engineer runs all of the diagnostic tests to verify that the new upgrade is operating as expected.
- 13** Sustaining Engineer informs Resource Manager that the upgrade is completed.
- 14** Resource Manager acknowledges the message from Sustaining Engineer and initiates host start-up commands.

- 15 Resource Manager, OP, and Sustaining Engineer receive message from HPOV that the host is back on-line.
-

Testing and Verification

Reboot

Rebooting each system following the installation of the operating system is required so that all operating parameters and variables are properly set. Note that there are two reboot procedures that follow, one for SGI, HP and Sun computers, the other for NCD computers.

Reboot Procedure for SGI, HP and Sun Computers

- 1 At the UNIX prompt for the workstation, type **su**, press **Return**.
 - 2 At the **Password** prompt, type **RootPassword**, press **Return**. Remember that **RootPassword** is case sensitive. You are authenticated as root.
 - 3 Type **who**, press **Return**. A list of users currently logged into the workstation appears.
 - 4 If users other than root and you are logged in:
 - type **wall**,
 - press **Return**,
 - type **The system is going down in 5 minutes for Reason. Please save your work and log off. We apologize for the inconvenience.**,
 - press **Return**,
 - press **Control-D**,
 - wait 5 minutes before proceeding to step 5.
 - 5 Type **/etc/reboot**, then press **Return**. The workstation reboots. Watch the status messages that appear for any errors. If you are returned to a **Login** prompt and saw no errors during the reboot, the reboot was successful. If the reboot was unsuccessful, use the error messages and system logs to figure out what is incorrect in the workstation installation. The system logs are: **/var/adm/messages** for Solaris 2.4/5.4, **/var/adm/SYSLOG** for IRIX 5.3 and 6.2, and **/usr/adm/syslog** and **rc.log** for HP-UX 9.05.
-

Reboot Procedure for NCD Computers

- 1 Press the **Setup** key. The **NCD User Services: Console** window will appear.

- 2 Go to the **Console** menu, select **Reboot**. The **Reboot** window opens asking if it is **OK to reboot the terminal**.
 - 3 Click the **OK** button. The NCD reboots. Watch the status messages that appear.
 - 4 Once the NCD successfully reboots, a login screen appears.
 - 5 If the NCD does not successfully reboot then use the information in the status messages to determine what went wrong in procedure 3.5.2.2.4 NCD Operating System Installation.
-

Logging In

Now that the hardware and software have been installed, it is time to log onto the workstation to assure that the user authentication system is operating properly.

Logging In Procedure

- 1 At the **Login** prompt for the workstation, type *YourUserID*, press **Return**.
- 2 At the **Password** prompt, type *YourPassword*, press **Return**.
 - Remember that *YourPassword* is case sensitive.
 - You are logged in and authenticated as yourself.
 - You are returned to a UNIX prompt.
 - If you are not logged in and returned to a UNIX prompt, logging in was unsuccessful. Follow these steps:
 - Execute this procedure one more time.

If logging in is unsuccessful again, there is a problem with the workstation installation. Continue to step b.

 - Type **root** at the **Login** prompt, press **Return**.
 - Type *RootPassword* at the **Password** prompt, press **Return**.

Remember that *RootPassword* is case sensitive.

You are authenticated as root and returned to a UNIX prompt.

 - Check that automount is running by typing **ps -ef | grep auto** or **ps -aux | grep auto**, press **Return**.

If automount is running then you will see output similar to this:

yourID	10173	0.2	0.4	648	408	pts/38	S	15:35:51	0:00	grep	auto
root	140	0.0	0.8	1796	1004	?	S	Jun 25	2:40	usr/lib/autofs/automountd	-D ARCH=sun5

If automount is not running then run it by typing:

- **/usr/lib/autofs/automountd -D ARCH=sun5** for Solaris 2.4/5.4,
- **/usr/etc/automount -D ARCH=sgi** for IRIX 5.3 and 6.2,
- **/usr/etc/automount -D ARCH=hp** for HP-UX 9.05,
- press **Return**.
- Try logging in again by typing **su - YourUserID**, press **Return**, type **YourPassword**, press **Return**. Type **whoami** and press **Return** to confirm that you successfully logged in as yourself and type **cd**, press **Return**, type **pwd**, press **Return** to confirm that you are in your home directory. If these commands return **YourUserID** and your home directory, you have successfully logged in. If you have not successfully logged in, proceed to step e.
 - The workstation probably did not successfully bind to a NIS server. Verify that the NIS server is up and on the network. Once it is, execute procedure 3.5.3.1 Reboot and then execute this procedure again.

Test Environment

The Test Environment procedure is performed to assure that the workstation is operating and is connected to the NIS.

Test Environment Procedure

- 1 At the UNIX prompt, type **ps -ef | more** or **ps -aux | more**. A screen full of information about the currently running processes is displayed.
 - 2 Look for the processes associated with the custom and COTS software which you installed in the process listing. To move to the next page full of information, press the **Space** bar. If a process is missing in the listing, go back to the installation of that software package to determine what went wrong.
 - 3 Type **cd ~/YourUserID**, press **Return**.
 - 4 Type **pwd**, press **Return**, use the output to verify that you are in your home directory. This verifies that automount is running and working correctly for the NIS map **auto.home**. You may follow steps similar to steps 3 and 4 for the other NIS maps. This also verifies that the new workstation was able to contact a NIS server.
-

Practical Exercises

Introduction

These practical exercises are presented in “day-in-the-life” scenarios relating to system administration activities. They represent real situations that you, as system administrator, are likely to encounter on a day-to-day basis.

Equipment and Materials

A functioning Pre-Release B Testbed computer system.

Document 456-TP-005-001, System Administration.

System Startup and Shutdown

- 1 Assume that the SQL server needs maintenance and has to be shutdown in a normal and routine fashion. Perform the actual steps that will accomplish this task.
- 2 Upon completion of the maintenance, the SQL server must be brought back on line again. Perform the actual steps that will accomplish this task.

Tape Operations, System Backup and Restore

You have received an approved request from the SEO Chief to perform an incremental backup of all the files in the **/etc**, **/vol0/admin**, and **/usr/bin** directories.

- 1 Estimate how many tapes it will take to back up the data.
- 2 Prepare the appropriate number of new tapes to accommodate the backup and perform the label and inventory operations on the tapes.
- 3 Perform the backup.
- 4 A user calls you and tells you that she has inadvertently erased three files (to be announced from the podium) that are critical to her research. She does not remember exactly when they are were last modified. Locate the latest versions of each of the files and perform a file restoration using the rename option for any conflicts that might arise.

User Administration

- 1 Add the following individual to the system:

UNIX User Registration Request

REQUESTER INFORMATION:

Name: Erica J.

Sonnenshein

Office Phone Number: (301) 999-

5555

E-Mail Address: esonnens@gsfc.nasa.gov

Office Location: Bldg. 32

NEW USER INFORMATION:

Name: Peter

Kovalkaides

Office Phone Number: (301) 555-

1234

Home Phone Number: (301) 444-

4444

Organization: GSFC

DAAC

Group Affiliation(s):

SMC

Role(s)/Job(s)/Justification: computer operator with database access required

Date of Request: 9/17/97

Date Required:

9/22/97

Supervisor Approval: _____ Date:

Ops Supervisor Approval: _____ Date:

- 2 The user you just added has called you with the news that she has forgotten her password. Describe the procedures you must follow to receive authorization to change the individual's password. Assuming you have received the appropriate authorizations, change the password to **gnu-Uzr**.
- 3 Change the group affiliations for this user to **adm**.
- 4 Ms. Sonnenshein sends you an e-mail message informing you that the work on her task is complete and requests that you change the access privileges on all files owned by her to READ ONLY for all classes of users to protect them from changes.
- 5 You have determined that space on the science processor is becoming rather scarce. There are a few large files (to be announced from the podium) that need to be deleted, and since Ms. Sonnenshein is done with her project, her home directory can be moved to the /tmp directory. Perform the procedures that will accomplish these tasks assuming you have received the appropriate authorizations. When you are done, inform the affected user of the changes.

Slide Presentation

Slide Presentation Description

The following slide presentation represents the slides used by the instructor during the conduct of this lesson.